¿ALGUIEN HACKEARA MI IPHONE?

NEX IT SPECIALIST #42

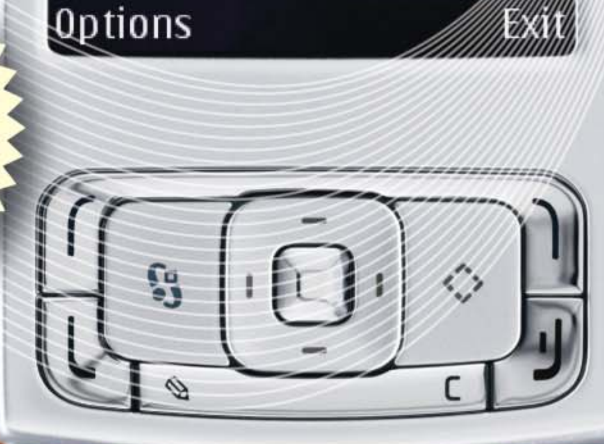


$10,80 EN TODO EL PAÍS

REVISTA DE NETWORKING Y PROGRAMACIÓN

#42

SMART PHONES por dentro



¿Hacia donde va el datacenter?



El arte de la virtualización según Xen

- SMARTPHONES POR DENTRO -

MANAGERS EN IT
Next Generation TCP/IP

NETWORKING
Comunicaciones Satelitales



WWW.NEXWEB.COM.AR
ISSN 1668-5423
Correo Argentino FRANQUEO A PAGAR Cta. 16185



DRAFTFCB
Nuevo Personal BlackBerry 8300.
Lleve su mundo a todas partes.
Personal.com.ar
Personal
BUENOS AIRES ARGENTINA YCA
CUSI 3
ROLEX
BlackBerry
12:21
WED, MAY 25
(3) Messages
• Internet
• Chat
• Email
12 cuotas de:
$108[25]
PRECIO FINAL: $1299
Personal BlackBerry 8300
Personal
Personal Empresas
Adquiéralo en nuestras Oficinas Comerciales.

NEX IT SPECIALIST - STAFF

DIRECTOR
- Dr. Carlos Osvaldo Rodríguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

COORDINACIÓN EDITORIAL
- María Delia Cardenal
- Carlos Rodríguez

SENIOR SECURITY EDITOR
- Carlos Vaughn O'Connor

DEPARTAMENTO DE VENTAS
- Ignacio Tellería
- Samanta Casado Arroyo

EDITORES TÉCNICOS
- Thomas Hughes
redaccion@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- Sabrina Furlan
- Florencia Mangiantini
- Carlos Rodríguez Bontempi

DISTRIBUCIÓN
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Ernesto Quirino
- Pablo Rivas
suscripciones@nexweb.com.ar

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Huesca Distribuidora de Publicaciones S.A. Aristóbulo del Valle 1556/58. C1295ADH - Capital Federal Argentina. (www.distribuidorahuesca.com.ar)
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1
C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar



Premio Sadovsky: Premio a la Trayectoria Periodística.

Hace 4 años nació NEX IT Specialist como un periódico de distribución gratuita. En estos años pasamos de formato periódico a una revista de pocas hojas, para finalmente y desde el #14 salir con el formato actual.
Quienes a diario hacen NEX hoy forman un team de redactores y diseñadores gráficos, quienes además tienen ahora la responsabilidad adicional del portal www.nexmedia.com.ar ("Saber de tecnología es saber de negocios").

Lo que nunca cambió en NEX es el estándar de sus artículos ni su objetivo: excelencia y enseñar respectivamente. Mantener al día con las novedades en tecnología a quienes ya forman parte del mundo de las TICs y enseñar a quienes buscan una salida laboral y se hallan en plena etapa de formación.

Nuestros redactores técnicos conforman un grupo muy selecto de expertos en desarrollo, infraestructura, comunicaciones o seguridad informática.

He sido postulado al premio a la trayectoria periodística de los premios Sadovsky y esto para mi como editor de NEX es un honor.
Como curiosidad me parece interesante contarles, que conocí hace ya varios años al Dr. Sadovsky cuando era secretario de Ciencia y Técnica en un proyecto muy ambicioso de conectar a los científicos argentinos con universidades e institutos de investigación del exterior y sus recursos de cómputo. Quizás un proyecto adelantado a su tiempo.

Esta postulación la deseo compartir con quienes trabajo a diario para hacer NEX. ●

Dr. C. Osvaldo Rodríguez
Editor,
NEX IT Specialist

LOS H

La confiabilidad que necesita

EDICIÓN ESPECIAL



Fundación Favaloro: de Linux a la confiabilidad de Windows Server

Con la plataforma integrada Microsoft, agilizó la carga de información, consolidó el monitoreo de las aplicaciones y ganó en seguridad y confiabilidad.

Después de migrar sus estaciones de trabajo y servidores que corrían sobre Linux a la nueva generación de Windows Server System, Windows XP y Office 2003, Fundación y Universidad Favaloro incrementaron su capacidad de transacciones y los niveles de confiabilidad de la plataforma informática. A su vez, redujeron significativamente los costos de administración de sistemas.

En 2005 las dos organizaciones dedicadas a la atención e investigación en cardiología, experimentaron un fuerte crecimiento tanto en cantidad de servicios médicos y pacientes como en volumen de facturación, lo que hizo colapsar su operatividad. La plataforma informática había llegado al límite de su capacidad de procesamiento de transacciones reduciendo así su posibilidad de interoperar con otros sistemas. Mientras la Fundación se manejaba con productos Microsoft, la Universidad tenía servicios basados en Linux. La decisión entonces fue implementar Windows Server System para contar con una plataforma integrada que incrementara la interoperabilidad y soportara aplicaciones críticas.

El Gerente de Sistemas de la Fundación, Sergio Navarro, señaló al respecto que la plataforma tecnológica resultó segura y confiable debido a que se lograron optimizar las funciones del sistema y del correo electrónico. "Además —agregó— nos permite usar nuestro sistema de gestión hospitalaria al máximo, con todas las prestaciones y funcionalidades de las últimas versiones, incluyendo soluciones antispam y antivirus."

Continúa en Pág. 3.

Las razones de la elección

"Para la institución fue muy importante elegir un socio tecnológico como Microsoft porque le permitió alcanzar una mayor disponibilidad de la plataforma, sin aumentar los costos de operación, ni los profesionales dedicados en el área de sistemas", comenta Gustavo Marota de TPS, Socio de Negocios certificado Microsoft que ayuda a la Fundación a afrontar sus desafíos tecnológicos.

Microsoft

ECHOS

para tomar sus decisiones

Para conocer más sobre este y otros casos visite http://www.microsoft.com/argentina/hechos
o llame al 0800-999-4617



FOTO: P. GONZALEZ



En primera persona

"Ahora tenemos una infraestructura informática mucho más confiable y segura para soportar nuestras aplicaciones críticas. Después de migrar el último servidor Linux a Exchange, no tendremos más servidores Linux en la institución."

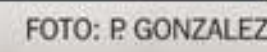
Sergio Navarro, *Gerente de Sistemas de Fundación Favaloro*

Excelencia en salud

La Fundación Favaloro es una entidad sin fines de lucro dedicada a la docencia, investigación y asistencia en el terreno de la salud, especialmente en cardiología y otras prestaciones de alta complejidad. Creada en 1975 por el Dr. René G. Favaloro, brinda soporte también a la Universidad. **Pág. 7**

Resultados tangibles

La solución consistió en migrar a Windows Server System (con Microsoft SQL Server 2000, Exchange Server 2003 e ISA Server 2004), Windows XP y Office 2003. Navarro señala que la organización logró aumentar la capacidad transaccional del correo en más de un 67%, y la base de datos en más de un 50%. **Pág. 15**



En pro de achicar la brecha digital





Bajo el lema "Laboratorio para el uso de metodologías innovadoras en la capacitación de IT para maestros de escuelas primarias", el Dr. C. Osvaldo Rodriguez, la Dra. Alicia Jubert, el Dr. Reinaldo Pis Diez, el Ing. Claudio Godoy y el Lic. Carlos Rodriguez junto con la Facultad de Ciencias Exactas de la Universidad Nacional de La Plata y Microsoft Research desarrollaron un proyecto de Inclusión Digital inaugurado en noviembre de 2007 el cual tiene como foco a la Escuela Especial #502 de Villa Elvira, La Plata.

El principal objetivo del proyecto es capacitar a los maestros de la escuela primaria en el uso de la tecnología. Para esto se montó el laboratorio con ocho PCs totalmente equipadas para que ejerciten con las diferentes herramientas y exploren las infinitas posibilidades existentes. La idea es que finalmente los docentes le puedan traspasar el conocimiento adquirido a sus alumnos y de esta forma incorporar a la tecnología en pro de la educación.

La primera clase, desarrollada en el marco de la inauguración, estuvo enfocada en lograr que los maestros tuvieran un contacto inicial con la computadora, se familiarizaran con ella y le perdieran el miedo. Con la tutoría del profesor de música de la Facultad de Bellas Artes de la Universidad de La Plata Mario Oriente Arreseygor, los maestros se convirtieron en alumnos.

El primer paso fue presentar un novedoso programa que ayuda en la composición de canciones mediante un pentagrama y notas musicales, muy usado por Arreseygor en la enseñanza de niños. La canción elegida: "Este puente se cayó". Cada uno de los maestros tenía frente a sí el software con el cual debían interactuar en tiempo y forma para lograr reproducir la melodía correcta. Para esto, cada golpe de la barra espaciadora significaba el toque de una nota, con lo cual se debía mantener el ritmo adecuado, regular los tiempos y las distancias para evitar lapsos de silencio y perder el compás.

El resultado fue asombroso. Las ganas y el miedo combinados hicieron que en un primer momento hubiera una total descoordinación, pero con el pasar de los pentagramas la melodía tomó su curso.

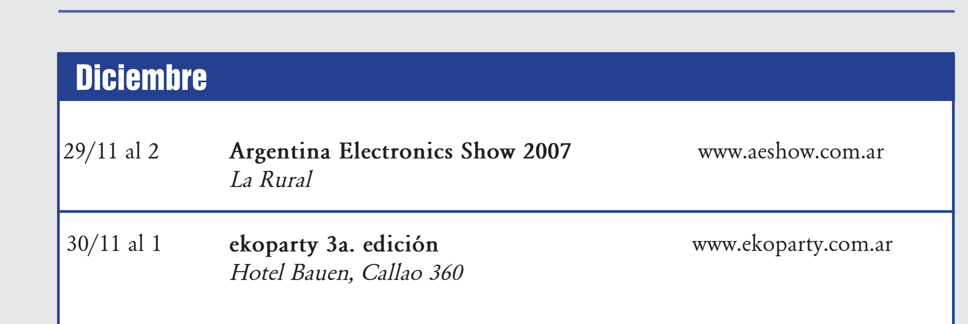
La idea no era que los maestros tuvieran una clase de música, sino que rompieran las barreras del miedo y sintieran que más que aprendiendo estaban jugando, excelente filosofía a aplicar con sus alumnos el día de mañana.

Una clase llena de música, cantos, risas, errores y aciertos fue el resultado de la primera experiencia del Laboratorio que promete continuar con la capacitación de maestros de otros establecimientos y lograr un efecto multiplicador.

¿Cuál es el valor de darle a los chicos de escuelas primarias laptops si sus maestros nunca usaron un procesador de texto o nunca enviaron un e-mail?







Diciembre

29/11 al 2	**Argentina Electronics Show 2007** *La Rural*	www.aeshow.com.ar
30/11 al 1	**ekoparty 3a. edición** *Hotel Bauen, Callao 360*	www.ekoparty.com.ar

PROTOCOLO DE ENRUTAMIENTO



■ Juan Manuel Urti
Ing. en Telecomunicaciones
I.U.P.F.A.

Introducción

En este artículo comenzamos a hablar de los protocolos dinámicos por estado de enlace. Los mismos han sido creados por el IETF, con el objetivo no solo de mejorar la performance y el rendimiento de los protocolos de Vector Distancia, sino que además han producido un cambio paradigmático, permitiendo realizar el escalamiento y dimensionamiento de una red IP, de una forma más ordenada.
Hasta el momento mencionamos RIPv1 y RIPv2, pero hemos dejado en evidencia que estos protocolos presentan una cantidad de problemas que han llevado a su desuso por parte de los administradores de red. Brevemente recordemos que RIP, en ambas versiones, posee un número máximo de saltos de 15 routers, además de que los updates de ruteo transportan, cada una cantidad regular de tiempo, la tabla de enrutamiento completa, produciendo que estos paquetes ocupen una cantidad importante del ancho de banda disponible de los enlaces. Otras desventajas, no menos importantes, son que este protocolo no permite segmentar la red en "áreas", dejando una topología de nivel 3 totalmente plana, y que además utiliza como métrica de decisión para hallar el camino más corto la cantidad de saltos, y no el ancho de banda u otro parámetro más útil para las redes de nueva generación.
A raíz de lo mencionado surgió OSPF -Open Short Path First-, promovido y creado por el IETF, que permite publicar rutas IP –solo IP- de una manera más eficaz. Este protocolo trabaja de la siguiente manera: crea un árbol de topología y adyacencias, para luego, a cada ruta publicada por un neighbor aplicarle un algoritmo conocido como Dijkstra, el cual halla la ruta más corta hacia el destino.
Las principales características de OSPF son las siguientes:

- Consiste en Sistemas Autónomos y áreas: al configurar se debe definir a qué área OSPF pertenece la interfase. Esto permite jerarquizar las redes.
- Soporta CIDR y VLSM: permite las máscaras de longitud variable y la utilización de súper redes.
- Minimiza el tráfico de update: sólo publica la tabla completa al iniciar el proceso, y además envía updates solo cuando la red cambia.
- Métrica mejorada: la métrica que se usa para elegir el mejor camino es el ancho de banda, permitiendo igualmente un número infinito de saltos.
- Publicación de updates: salvo al comienzo, el resto de los updates se emiten solo cuando se produce un cambio en la red. Se realiza por medio de Multicast a la dirección IP 224.0.0.5.

Áreas OSPF

A pesar de que OSPF no es habitualmente utilizado para comunicar diferentes Sistemas Autónomos, puede ser empleado para tal fin con

FOTO: http://www.sxc.hu/ - Tony Clough

PROTOCOLO SPF

En este artículo de la serie explicaremos el primer protocolo dinámico de estado de enlace. Este tipo de protocolos envían por medio de paquetes periódicos el estado de las interfases y sus características. Hoy en día, OSPF es uno de los protocolos de LAN y WAN más empleados, debido a que soporta una gran cantidad de rutas.



"El **OSPF** - Open Short Path First - permite publicar rutas IP - sólo IP - de una manera más eficaz, el cual crea un árbol de topología y adyacencias, para luego, a cada ruta publicada por un neighbor aplicarle un algoritmo conocido como Dijkstra, el cual halla la ruta más corta hacia el destino".

Figura 1- Sistema Autónomo



el objetivo de separar dominios a la hora del diseño. Igualmente para realizar esta acción, es que el protocolo permite la división de la red en áreas, que son redes más pequeñas en las que los routers se comunican los updates solo entre ellos, evitando que en redes muy grandes, el proceso de convergencia sea extremadamente complejo. Esto conlleva la ventaja adicional de que reduce aún más el overhead producido por el tráfico de update, y además confina la inestabilidad de la red a cada área, sin que afecte a la vecina.
Cada área posee un ID, y debido a que un router puede pertenecer a varias áreas, el ID es asociado a una interfase a los fines de poder diferenciar la membresía.
Dentro de esta segmentación de las redes, cada área esta obligada a estar comunicada con la denominada "área 0", también conocida como Backbone. A continuación podemos observar un AS, divido en 3 áreas, en las cuales cada router posee un nombre específico en virtud de su función.
De la figura 1 podemos explicar la función de cada router. Los routers Autonomous System Boundary Routers -ASBR- son los elementos de nivel 3 que están en el Backbone. Por pertenecer al área 0 conectan múltiples routers que se encuentran en diferentes áreas, ya que recordemos mencionamos que todas las áreas deben estar al menos conectada al Backbone. Los Area Border Routers -ABR- son routers, que conectan a un área con el Backbone, teniendo al menos una interfase conectada a este. Dividiendo de esta manera la red, permitimos que los updates de ruteo se mantengan dentro de cada área, evitando crear inestabilidad a la totalidad del segmento.

Base de datos de la Topología

Esta base de datos contiene toda la información recibida por los vecinos, y se emplea como datos de entrada a la hora del calcular el árbol, aplicando el algoritmo de Dijkstra. Esta información se recibe vía los Link State Advertisement -LSA-, que contienen el estado de los enlaces y la información de enrutamiento compartida.
Entendamos por enlace, una interfase que participa en el proceso de enrutamiento dinámico, en la que el LSA publica su estado (up o down) y también su dirección IP.
Cuando dos routers poseen una interfase en la misma subred que otros, o bien están directamente conectados, se transforman en neighbors o vecinos. La Tabla de Neighbors mantiene una descripción de cada router con el cual se ha creado una adyacencia.
Recuerde que todos los routers que están en la misma área poseen la misma base de datos de la topología.

Funcionamiento de OSPF

A continuación daremos una breve explicación de cómo funciona OSPF, advirtiendo al lector que para profundizar ahonde la bibliografía especializada en el tema, la cual es variada y amplia.
OSPF emplea un protocolo llamado "Hello" para descubrir neighbors o vecinos, enviando periódicamente un paquete multicast a la IP 224.0.0.5. De esta manera nos aseguramos que todos los routers que permitan el proceso OSPF se hagan conocer a sus vecinos. Una vez conocido, el router debe formar adyacencias con los demás dispositivos de nivel 3. Una adyacencia es una relación entre dos routers que corren OSPF y que intercambian directamente información de enrutamiento. Los routers solo intercambian información con aquellos otros dispositivos de la red con la que hayan creado una adyacencia, a diferencia por ejemplo EIGRP que lo hace con todos los del AS.
En las redes del tipo broadcast y Non broadcast Multiaccess, como lo son respectivamente las redes Ethernet y Frame Relay, para minizar el número de adyacencias se designan dos roles fundamentales: el Designated Router –DR- y el Back up Designated Router –BDR-.
El DR es elegido en virtud del Router ID –RID-, que habitualmente es la IP

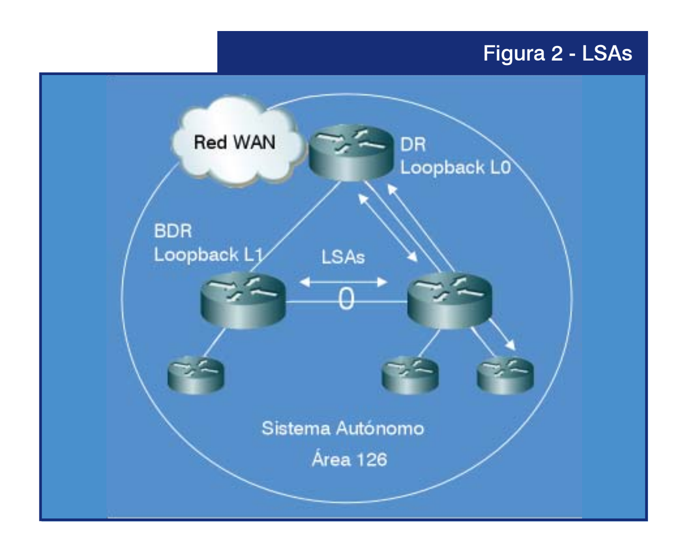
más alta configurada en alguna interfase física, o bien puede tomar como prioridad alguna IP de Loopback configurada en el equipo, con el objetivo de mantener al DR estable en la red (siempre se toma la Loopback antes que cualquier otra IP). El BDR es elegido con el mismo criterio.
El objetivo de manipular al DR por medio de una interfase loopback es tratar de seleccionar los routers que se encuentren en el borde del área.
Las funciones principales del DR son: crear adyacencias con todos los routers de la misma área, recibir y enviar los updates de ruteo y los LSA, permitir que la tabla de topología de todos los routers esté sincronizada.
El BDR es un DR en stand by, que también recibe todos los updates, pero no inunda la red con los LSA, ya que es tarea del DR. De lo mencionado debe quedar claro que los LSA fluyen, en este tipo de redes, solo entre los routers remotos y los DR y BDR, no habiendo LSA entre otros routers que pertenezcan a la misma área.

Cálculo del Árbol

Para hallar el camino más corto, cada router debe calcular el mejor camino hacia cada destino dentro de su misma área, y ello es posible gracias a la base de datos de la topología, la cual se fue formando gracias a los LSA provenientes del DR. Luego de esto, y obviamente luego de aplicar el algoritmo, cada router creará un árbol en el cual el mismo será la raíz del árbol, y cada rama será un camino hacia una subred.
El costo hacia una red es calculado en virtud a la sumatoria de los anchos de banda de los enlaces intermedios. Esto está definido en la RFC 2338, que aunque no especifica el valor exacto, deja sentado que el BW es la métrica a emplear en OSPF. ●

"Si un router pertenece a varias áreas, debe crear varios árboles, uno por cada área".

Figura 2 - LSAs



Miguel F. Lattanzi
Ing. en Telecomunicaciones (IUPFA)

SERVICIOS SATELITALES



Entre las aplicaciones más comunes se encuentran la adquisición de imágenes y los servicios de telecomunicaciones. Muchas de las tareas que se realizan en la actualidad serían imposibles de realizar sin los satélites.

Evolución Histórica

La historia de los sistemas satelitales actuales comienza el 4 de octubre de 1957, cuando la ex Unión Soviética lanzó y colocó en órbita el primer satélite artificial –creado por el hombre- de la historia, llamado ISZ (Satélite Artificial Terrestre, del idioma Ruso) conocido popularmente como Sputnik I. Éste fue el primero de una serie de satélites correspondientes al programa espacial Sputnik.

El Sputnik I tenía una masa aproximada de 83 Kg., contaba con dos transmisores de radio que operaban a 20MHz y 40MHz. Su órbita estaba ubicada a 938 Km de altura en su apogeo y a 214 Km. de altura en su perigeo, con respecto a la superficie terrestre.

Por su parte, Estados Unidos también trabajó sobre los satélites por medio de la U.S. Navy (Marina de los Estados Unidos) con la implementación del Proyecto Vanguard. El primer lanzamiento de este proyecto se intentó antes que el Sputnik, pero resultó fallido por problemas técnicos.

Dada la importancia estratégica y política que suponía para la época este tipo de cuestiones, se enfocaron la mayoría de los recursos destinados a investigación espacial al Programa Júpiter del U.S. Army (Ejército de los Estados Unidos).

Los objetivos de este proyecto quedaron satisfechos por medio del lanzamiento exitoso del Explorer 1, el 31 de enero de 1958.

Este evento es considerado hoy en día como el desencadenante en la carrera espacial entre las dos superpotencias, Estados Unidos y la ex Unión Soviética.

Los lanzamientos que se realizaron en la década del ‘50 fueron los impulsores de los actuales sistemas satelitales y sirvieron como ensayo para los desarrollos futuros que se realizarían en los años siguientes.

FOTO: http://www.sxc.hu/ - Arno Enzerink

Los ‘50 fueron testigos de los siguientes lanzamientos exitosos:

04-10-1957 Sputnik 1 - USSR
03-11-1957 Sputnik 2 - USSR
31-01-1958 Explorer 1 - USA
05-03-1958 Explorer 2 - USA
17-03-1958 Vanguard 1 - USA
15-05-1958 Sputnik 3 - USSR
11-10-1958 Pioneer 1 - USA
02-01-1959 Luna 1 - USSR
03-03-1959 Pioneer 4 - USA
12-09-1959 Luna 2 - USSR
04-10-1959 Luna 3 - USSR

A principios de 1960, la American Telephone and Telegraph Company (AT&T) publicó estudios indicando que unos cuantos satélites de gran capacidad y de diseño avanzado, podían soportar más tráfico que toda la red terrestre de AT&T de larga distancia.
El costo de estos satélites fue estimado en solo una fracción del costo de las facilidades de microondas terrestres equivalentes, necesarias para manejar la misma cantidad de tráfico. Desafortunadamente, debido a que AT&T era un proveedor de servicios y no de tecnología, los reglamentos del gobierno de Estados Unidos le impedían desarrollar los sistemas satelitales necesarios. Por lo cual otras empresas ocuparon el lugar, comenzando así la carrera por el desarrollo de satélites.
A través de los años, los precios de la mayoría de los bienes y servicios han aumentado sustancialmente, sin embargo los servicios de comunicación por satélite se han vuelto más accesibles cada año. En la mayoría de los casos, los sistemas satelitales ofrecen más flexibilidad que los cables submarinos, cables subterráneos, enlaces de microondas y sistemas de fibra óptica.

Características y Funcionamiento de un Sistema Satelital

Un sistema satelital básico debe tener un satélite (correspondiente al segmento espacial o satelital), una estación terrena (correspondiente al segmento terrestre) para controlar su funcionamiento y una red de usuario final, cuyas características estarán directamente relacionadas con el servicio que esté prestando el sistema satelital en cuestión.

Como puede verse en la figura 1, existen básicamente tres tipos de órbitas para el posicionamiento de satélites alrededor de la tierra. Una es la llamada Órbita Baja o LEO (Low Earth Orbiting) que se encuentra aproximadamente entre los 400 Km. y 1.400 Km. de altura con respecto a la superficie terrestre a nivel del mar. Otra posición disponible es la conocida como Órbita Media o MEO (Medium Earth Orbiting), esta se encuentra entre los 10.000 Km. y los 20.000 Km. con respecto al nivel del mar. Por último están los satélites de Órbita Geoestacionaria o GEO, estos orbitan a una altura aproximada de 36.000 Km. y tienen una velocidad nula con respecto de la tierra.
Un componente fundamental del sistema es la estación terrena, la misma es un conjunto de equipos de comunicaciones y de procesamiento de datos que puede ser terrestre fijo o móvil, marítimo o aeronáutico. Las estaciones terrenas pueden ser usadas en forma general para transmitir y recibir señales, hacia y desde el satélite.
Éstas varían según su diseño, dependiendo si se utilizan para transmitir o recibir señales, el tipo de señales en uso y la intensidad de la señal recibida.
El principal componente dentro de la sección de subida, de un sistema satelital, es el transmisor de la estación terrena.
El satélite tiene uno o varios transponder (dispositivo emisor-receptor).

Un típico transponder satelital consta de un dispositivo para limitar la banda de entrada, un amplificador de bajo ruido de entrada, un transductor de frecuencia, un amplificador de potencia de bajo nivel y un filtro pasa-banda de salida.

El funcionamiento básico de un Sistema Satelital es el siguiente, una estación terrena que está bajo la cobertura de un satélite le envía una señal de microondas, denominada enlace ascendente o Uplink. Cuando éste la recibe, el transponder del satélite simplemente la retransmite a una frecuencia más baja para que la capture otra estación, lo que se denomina enlace descendente o Downlink.
El trayecto que recorre la comunicación para el caso de un satélite geoestacionario es de unos 70.000 Km. y sólo le toma alrededor de 1/4 de segundo cubrir dicha distancia, por tanto una comunicación bidireccional en estas condiciones tendría un retardo de 1/2 segundo.

Los satélites pueden prestar una gran cantidad de servicios, entre los más comunes se encuentran los servicios de comunicaciones, obtención de datos para estudios meteorológicos, monitoreo de catástrofes ambientales, posicionamiento para navegación y obtención de imágenes.

Servicio de Comunicaciones

Hoy en día, los más importantes y utilizados son los satélites que brindan servicio de comunicaciones. Dentro de estos servicios se encuentran los de telefonía fija, telefonía móvil, fax, servicios de TV, transmisión de radio, etc.
Estos servicios permiten una transmisión rápida y segura alrededor de la tierra, los servicios de comunicaciones son muy importantes en la navegación marítima, que junto con los satélites de posicionamiento permiten a las empresas tener sus barcos comunicados y saber la ubicación precisa de cada uno de ellos, las compañías petroleras hacen uso extensivo de estos sistemas en conjunto para el control de sus flotas.
Los sistemas satelitales de comunicaciones han dado un nuevo impulso a la televisión, dado que pueden realizarse transmisiones en directo desde cualquier punto del planeta hacia otro. Además este tipo de soluciones permite desplegar y brindar rápidamente un servicio de TV en zonas donde no existe una infraestructura terrestre previa, como ser el caso de las operadoras tradicionales de TV por cable.

Servicio de Posicionamiento

Los dos sistemas existentes y en uso en la actualidad son el Sistema de Posicionamiento Global o GPS y el sistema GLONASS, siendo estos de Estados Unidos y Rusia respectivamente.
Estos sistemas permiten, por medio de un Terminal en tierra, saber la ubicación sobre la superficie terrestre y la altura de dicha ubicación. Los mismos están restringidos con una mayor precisión para uso militar, mientras que para uso civil tienen una precisión de ubicación de varios metros, así y todo son de gran ayuda para un infinito número de actividades.
Existe un proyecto de la Comunidad Europea para realizar una nueva red de posicionamiento independiente de las redes GPS y GLONASS, este proyecto se conoce como GALILEO.
El sistema GALILEO pretende resolver varias falencias de los dos sistemas existentes en la actualidad y además, a diferencia de estos, estará controlado por operadoras civiles que garantizarán determinados grados de seguridad requeridos por los gobiernos que intervienen en el proyecto.

Servicio de Adquisición de Imágenes

Otro tipo de satélite que ha tenido gran importancia en estos últimos años es el utilizado para realizar la adquisición de imágenes fotográficas de la tierra, esto ha dado lugar a muchos sitios de INTERNET especializados y a un nuevo rubro comercial. Este servicio se está haciendo cada vez más importante, a nivel científico, militar y comercial. El mismo permite la visualización de los diferentes puntos geográficos del planeta, pudiendo obtener imágenes de ciudades para realizar estudios demográficos o geográficos y la obtención de imágenes de ciudades, monumentos y edificios históricos y maravillas de la naturaleza con fines comerciales.
Los dos sistemas más conocidos son el Google Earth y el Ikonos, siendo este último de carácter más comercial y capaz de obtener imágenes a demanda.

La figura 2 muestra la comparación entre dos capturas realizada en Sumatra antes y después del Tsunami que azotó Asia en el 2004.

Conclusión

Hoy en día se están llevando a cabo proyectos para poder medir la contaminación ambiental, los cambios en los océanos, para llevar a cabo estudios de suelos, etc.
Está claro que los sistemas satelitales han tenido un impacto directo en la sociedad, desde el entretenimiento hasta el ámbito científico, es por ello que es de vital importancia continuar desarrollando este tipo de tecnologías con fines pacíficos. ●

Fig 1. Componentes de un Sistema Satelital

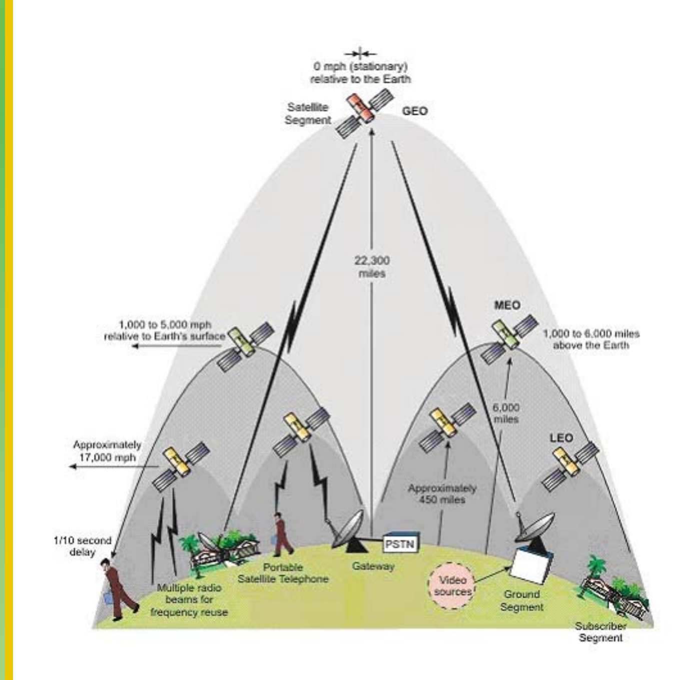


Fig 2. Imagen obtenida por el sistema Ikonos



SMART por dentro

Teléfono, agenda de contactos y reuniones, acceso al e-mail y a la web y la posibilidad de manejar documentos. Todo en uno. Son los ya conocidos SmartPhones que hoy en día ayudan a más de un profesional que debe estar la mayor cantidad del tiempo conectado.

Hay dos cosas que hoy en día son fundamentales para la mayoría de los profesionales: el celular y la computadora. Todos conocemos qué es lo que cada uno de estos dispositivos nos ofrecen y cuáles son sus limitaciones. Es por esto que no es de extrañar que se haya evolucionado hasta lograr un híbrido entre estas dos tecnologías. Son los bien conocidos Smartphones o teléfonos inteligentes.

En un principio se los pensó como una herramienta pura y exclusivamente para los profesionales y los hombres de negocio, pero luego todo tipo de consumidores empezaron a elegirlos. Los Smartphones combinan la inteligencia de las PDA y del celular en un mismo gadget, ofreciendo la posibilidad de no dejar de estar conectado con sus contactos, organizar sus reuniones, trabajar sobre documentos y más.

En la actualidad existen varios tipos de Smartphones en el mercado, encontrará modelos que hacen foco en las características de celular mientras que otros le dan más importancia a la mensajería. Esto generalmente influye en el diseño del smartphone, el que varía desde un dispositivo elegante hasta uno tosco.

Además, existe una variedad de sistemas operativos -Palm, Windows Mobile, Symbian, BlackBerry y Apple- cada uno con sus pros y sus contras.

Desde el principio

No existe hoy por hoy una definición cerrada de lo que es un smartphone o de las características que estos deben tener. Sin embargo para David Wood, EVP de Symbian, "los teléfonos inteligentes se diferencian de los celulares ordinarios por dos características: cómo están construidos y qué es lo que pueden hacer".

Muchos de los dispositivos considerados como smartphones utilizan en la actualidad un sistema operativo bien definido con la posibilidad de agregarle aplicaciones como procesamiento de datos, conectividad y entretenimiento.

En cuanto a sus características, la mayoría de estos teléfonos tienen acceso a Internet, al e-mail y a la agenda personal, muchos incluyen una interface adicional como un teclado QWERTY miniatura, pantalla táctil, cámara incorporada, administración de contactos, acelerómetro, programas de navegación y la posibilidad de ver documentos de Office y en formato PDF, como así también ver fotos, videos, escuchar música y acceder al e-mail corporativo.

El primer Smartphone fue diseñado por IBM en 1992 y puesto a la venta recién un año después. Además de tener las características propias de un teléfono celular, contenía calendario, agenda de direcciones, hora mundial, calculadora, note pad, acceso al e-mail, la posibilidad de enviar y recibir fax y juegos. Este teléfono no tenía un teclado físico sino una pantalla táctil por medio de la cual los usuarios seleccionaban los números de teléfonos y el texto se ingresaba a través de un teclado predictivo.

Con el correr del tiempo muchos celulares fueron presentados como "teléfonos celulares" pero sin realmente serlos.

PHONES



> Los **Smartphones** combinan la **inteligencia de las PDA** y **del celular en un mismo gadget**, ofreciendo la posibilidad de **no dejar de estar conectado** con sus contactos, **organizar sus reuniones, trabajar sobre documentos y más**

Por dentro

Los teléfonos inteligentes soportan una variedad de sistemas operativos entre los cuales se destacan:

• **Symbian OS de Symbian Ltd.:** Tiene acaparado el 72.4 por ciento del mercado y es adoptado por varias marcas como Nokia, Motorola, Samsung, LG.

• **Linux:** Tiene el 13.3 por ciento del mercado. Es muy fuerte en China donde está presentado por Motorola. En vez de ser una plataforma por si sola, Linux es utilizado como base de diferentes plataformas desarrolladas por los vendors.

Características	Apple iPhone	Nokia N95	Samsung Blackjack	BlackBerry Curve 8300	Palm Treo 750
Grosor	11.6 mm	21 mm	11.7 mm	15.5 mm	22 mm
Tam. de pantalla	8.9 cm	6.6 cm	5.6 cm	6.35 cm	6.35 cm
Material del Visor	Vidrio	Plástico	Plástico	Plástico	Plástico
Wi-Fi	Sí	Sí	No	No	No
Tiempo disponible para hablar	8 horas	4 horas	5.5 horas	4 horas	4 horas
Tiempo de uso de Internet	6 horas	No especifica	No especifica	No especifica	No especifica
Duración de video	7 horas	No especifica	No especifica	No especifica	No especifica
Duración de audio	24 horas	No especifica	No especifica	No especifica	No especifica

• **Windows Mobile de Microsoft:** Tiene el 6.1 por ciento del mercado. Tanto Windows CE como Windows Mobile están bastante difundidos en Asia.

• **RIM BlackBerry:** Tiene el 5.3 por ciento del mercado. Este sistema operativo es simple de operar y fue diseñado especialmente para los negocios aunque en la actualidad ha tenido muchas mejoras en lo que es entretenimiento multimedia.

• **Palm OS de PalmSource:** Tiene el 1.6 por ciento del mercado.

• **OS X de Apple:** Con el 1.3 por ciento del mercado. El iPhone utiliza un sistema operativo derivado del Mac OS X y no permite que otros programas le sean instalados, a menos no de forma legal.

A no confundir

Los teléfonos inteligentes, las PDAs y las Ultra-Mobile PC son cosas diferentes. Las Personal Digital Assistants son computadoras de mano con aplicaciones como calculadora, reloj y calendario, acceso a Internet y al e-mail, posibilidad de grabar videos, procesador de texto y de hojas de cálculos, libreta de direcciones, juegos de computadoras, GPS, la posibilidad de escuchar música o radio y sincronizar la información con la PC. Muchos PDAs además tienen pantallas color y muy buena resolución de audio y video, navegador de Internet a través de Wi-Fi o WWANs (Wireless Wide-Area Networks) y muchos tienen tecnología de touch screen.

Por otro lado existen las llamadas Ultra-Mobile PC, una pequeña computadora móvil de pantalla táctil, más grande que una PDA pero más pequeña que cualquier Tablet PC.

La primera generación de UMPC corría Windows XP Tablet PC Edition y fue duramente criticada por no tener un rumbo fijo. Parte del problema fue encontrar a sus usuarios: Microsoft sabía que quería desarrollar una computadora portátil de casi 18 centímetros de pantalla y un peso total menor a 1.3 Kg., pero no tenía en claro a qué audiencia estaría orientada.

Es por esto que la primera generación de UMPC llegó a los usuarios más entusiastas -gracias a la gran campaña de marketing-

¿Se viene el Gphone?

Todo lo contrario. Finalmente Google anunció el lanzamiento de una plataforma abierta para teléfonos móviles de nombre Adroide.

Junto con Motorola, Qualcomm, Telefónica, Telecom Italia, T-Mobile, HTC y Samsung, entre otras 34 empresas conformaron la alianza Open Handset para desarrollar un sistema operativo, middleware y una interfaz de usuario y aplicaciones para móviles la cual estará disponible para mediados de 2008.

"Con esta plataforma harás cosas con tu móvil que no podías hacer hasta ahora", afirmó Eric Schmidt, presidente y director ejecutivo de Google en el anuncio. Entre ellas, los usuarios podrán acceder a los servicios de Google -el buscador de Internet, Google Maps, Gmail, entre otros,- desde cualquier teléfono móvil y sin necesidad de estar frente a la computadora. Además, una de las mayores revoluciones, es que toda la información estará en la red en vez de en la computadora, por lo que se podrá acceder a ella en cualquier momento y en cualquier lugar.

Lo que resta saber es cómo reaccionarán los demás sistemas operativos -Windows Mobile, Palm, Symbian, BlackBerry y Apple. ¿Lo pasarán mal? ¿Competirán cabeza a cabeza? ¿O decidirán unirse a la Open Handset Alliance?

"¿Cuál es el **tamaño exacto** que debiera tener un **teléfono inteligente** para que combine lo **mejor de los dos mundos**?

He aquí la pregunta fundamental"

pero demostró ser un error, no llegó a cubrir las expectativas de ventas cuando fue lanzado a principios de 2006.
Sin embargo, el objetivo de Microsoft era crear un software fácilmente adaptable a las manos de un adulto llamado La Experiencia Origami, con los pros y los contras de Windows XP y Vista.
La principal ventaja de la UMPC es que es una computadora real. Corre Windows XP Tablet PC Edition 2005 o Windows Vista Home Premium Edition, o Linux y tiene un microprocesador Intel Pentium de voltaje ultra bajo, corriendo en el rango de 1 GHz y se la puede utilizar en la mayoría de las situaciones ya que no requiere de mucho espacio. La vida de la batería es bastante larga y a la altura de la de cualquier notebook tradicional. El teclado, si bien no es lo más cómodo que existe, es suficiente como escribir un mail, navegar por Internet y editar archivos de texto.
Sin embargo, aún existen varias cuestiones en las que trabajar. Probablemente la UMPC no sea utilizada como la única PC por la preocupación de su performance y de su tamaño. Si bien los viajeros ven como sumamente atractivo la posibilidad de poder desplazarse de un lugar a otro de manera más liviana, para aquellos que tienen una real necesidad de escribir y utilizar constantemente el teclado la UMPC no es lo ideal.
Existen varios modelos diferentes de UMPC donde las más poderosas tienen 1 GB de memoria hasta 256 Mb y todas con hasta 7 pulgadas de pantalla. Entre ellas la R2H de Asus, la Q1 Ultra de Sansung, y la VAIO UX180P de Sony.

¿Hasta dónde llega la comodidad?

Una de las características propias de los smartphones es el tener todo en uno y dejar de lado la necesidad de tener que acarrear con varios dispositivos a la vez, lo que en determinados momento resulta bastante molesto. Celular y PC todo en uno. Pero sabemos que un teléfono móvil cuanto más chico es más cómodo para trasladarlo; y una PC debe tener un tama-

¿Y el iPhone?



El último lanzamiento de Apple es el mundialmente conocido iPhone, el cual combina tres productos en uno: un teléfono móvil, un iPod de pantalla wide con controles táctiles, y un centro de conexión a Internet con servicio de correo electrónico con características de computadora de escritorio, navegador de web, buscador y mapas.

"Multi-touch"

Es uno de los cambios más grandes: este celular no tiene un teclado como los que estamos acostumbrados a ver. El iPhone presenta una nueva interfaz basada en una amplia pantalla táctil (multi-touch display) y un innovador software que le permite a los usuarios controlar absolutamente toda la pantalla con el solo toque de los dedos. Es decir que uno puede deslizarse entre las diferentes tapas de los cd, ver fotos y enviarlas por email con un solo toque, y hacer zoom in o zoom out en una parte determinada de una web page con los dedos gracias a la tecnología del multi-touch.

Wireless

iPhone usa quad-band GSM, el estándar mundial en comunicaciones wireless. Tiene 802.11b/g Wi-Fi, lo que da una gran velocidad de browsing y conectividad, y Bluetooth 2.0 con EDR (Enhanced Data Rate).

Sensores Avanzados

iPhone incluye avanzados sensores -un acelerómetro, un sensor de proximidad y otro de luz ambiental- los cuales detectan cuándo el usuario ha rotado el dispositivo de posición vertical a horizontal para cambiar automáticamente los contenidos de acuerdo con la posición de pantalla, y cuándo el usuario lleva el dispositivo al oído para inmediatamente apagar la pantalla y ahorrar energía y prevenir involuntarias aplicaciones por el contacto con la piel.
El sensor de luz ambiental automáticamente ajusta la luz del iPhone dependiendo de la cantidad de luz en el ambiente, mejorando la experiencia del usuario y, al mismo tiempo, ahorrando energía.

Internet

Lo que se destaca del iPhone es un rico cliente de email HTML y el Safari, el web browser más avanzado de un dispositivo móvil, que sincroniza automáticamente los bookmarks de la PC o Mac y permite que las páginas web se vean de la forma en la que fueron diseñadas para ser vistas. Además, es totalmente multi-tasking, permitiendo la lectura de una página web mientras se bajan los emails. Además presenta los Widgets, pequeños programas que toman determinada información de Internet como ser el estado del clima, reportes de acciones, etc.

ño mínimo para que se puedan utilizar con comodidad todas sus funcionalidades. Por lo tanto, ¿cuál es el tamaño exacto que debiera tener un teléfono inteligente para que combine lo mejor de los dos mundos? He aquí la pregunta fundamental.

Una de las críticas más fuertes hacia estos nuevos dispositivos es la incomodidad del tipiado. Cuando lo que uno necesita es navegar por la Web, escribir algún mail corto o ingresar un contacto a la agenda, el tamaño del teclado no será problema. Ahora cuando uno ya requiere utilizar el smartphone como una alternativa a la PC en viajes o trayectos largos y debe utilizar el procesador de texto o planillas de cálculos o características donde es imprescindible la posibilidad de tipiar cómodamente, lo mejor será recurrir a algún otro dispositivo.

De todas formas si lo que se requiere es un celular que además nos pueda mantener conectados para chequear e-mails, manejar la agenda de contactos y de ser necesario manejar algún documento el smartphone es lo ideal. Si necesita de una mayor comodidad, capacidad de procesamiento, velocidad y funcionalidades será mejor mantener su celular por un lado y optar por alguna alternativa. ●

Los SmartPhone y la medicina

Los países en desarrollo en la actualidad evidencian un gran crecimiento de su población, por lo que el Departamento de Desarrollo Internacional del Reino Unido (DFID) estima que para 2030 dos mil millones de personas estarán viviendo en malas condiciones: sin acceso a salud, educación o servicios sanitarios. El uso apropiado de información móvil y de la tecnología de la información, hablando del software tanto como del hardware, tienen el potencial para mitigar algunos de estos problemas que aumentan día a día.

Los smartphones que ya están en el mercado hace un tiempo son el resultado de la combinación de las funcionalidades de un PDA con las capacidades de un teléfono celular. Corren sobre una variedad de sistemas operativos y varios de ellos permiten la conexión a redes Wi-Fi. Como todo dispositivo tiene sus limitaciones pero ciertos casos un teléfono inteligente es más que útil.

Un ejemplo de ello es la aplicación de estos celulares en la medicina. El Northeast Medical Center Hospital de Estados Unidos decidió equipar a 30 de los 300 médicos con un smartphone para que pudieran acceder al sistema del hospital y a la información médica. De esta forma los profesionales pueden ingresar al sistema información crucial del paciente sin necesidad de abandonar las rondas médicas y realizarle una consulta a un colega mientras está con el paciente. De la misma forma si el médico realiza una visita médica a domicilio. Es así que se evita el tener que estar con dos dispositivos a cuestas y no se corre el riesgo del olvido de alguno de ellos.

En la actualidad se están desarrollando muchas aplicaciones para el mundo de la medicina. Entre ellas una que mida la presión arterial y los latidos del corazón y envíe esta información directamente a la base de datos de la organización para evitar que se acumule en el dispositivo. De esta forma se puede acceder a los datos en el momento en que se lo requiera.



Combinan lo mejor del mundo de los celulares y de las computadoras. Veamos cuáles son los teléfonos inteligentes más populares y qué nos ofrece cada uno.







HP iPAQ 510 Voice Messenger

- Dimensiones: Peso :100 g / 10.5 cm x 4.85 cm/ Profundidad: 1.65 cm.
- Capacidad: Memoria Instalada 64.00 MB / Terminales de Memoria / Tarjeta microSD. / Ranura para Micro SD que admite memoria microSD de 4 bits estándar.
- Display: Pantalla TFT transflectiva de 2,0 pulgadas, a color con 176x220 píxeles y luz de fondo con LED.
- Sistema Operativo: Microsoft Windows Mobile 6.0.
- Camara: 1.3 Megapixels / Profundidad de color.
- Conectividad: WIFI - 11 Mbps IEE E802.11b / WIFI - 54 Mbps IEEE802.11g/ Versión USB 1.1 (Hasta 1.5 MB/s).
- Batería: Batería (tiempo en conversación) 6 hr / Batería (tiempo en standby) 7.8 d / Capacidad de la batería 1100 mAh.
- Audio: Micrófono, receptor, altavoz integrados y un conector de auriculares estéreo de 2,5 mm, estéreo (a través del conector de auriculares).
- Funciones: Adaptador AC. / Cable USB / Cargador / SMS / EDGE / GPRS / HTML / Tecla de navegación de 5 vías, 2 teclas de software, enviar/fin, principal, volver, control de volumen, comando de voz y teclado alfanumérico de 12 teclas

FOTO: http://www.sxc.hu/ - linusb4





iPHONE

- Dimensiones: 115 mm x 61 mm / Profundidad: 11.6 mm / Peso: 135 gramos.
- Capacidad: 4 GB u 8 GB flash drive.
- Display: 3.5 pulgadas (diagonal) widescreen multi-touch display / 480 by 320 pixel resolution at 163 ppi / Soporte para display con multiples lenguajes y caracteres simultaneamente / pantalla multitáctil / Acelerómetro que detecta si el dispositivo está en posición horizontal o vertical (2D).
- Sistema operativo: OS X / GSM / Cuatribanda (850, 900, 1800, 1900 MHz).
- Wireless data: Wi-Fi (802.11b/g)/ Bluetooth 2.0.
- Camara: 2.0 megapixels.
- Video: Stereo audio in .m4v, .mp4, and .mov file formats.
- Bateria: Recargable. Bateria de litio-ion / Tiempo en conversación: + de 8 hs / Tiempo en espera: + de 250 hs / Internet: + de 6 hs / Video: + de 7 hs / Audio: + de 24 hs.
- Funciones: push e-mail / telefonía móvil / mensajería de texto / navegación web con Safari. / Control de Volumen Up / Down / Timbre / modo Silencio- Boton Power / Lock / Sleep / Wake- Boton de Menu o Home.
- MP3: La parte del iPod presenta una interfaz con portadas flotantes y efectos 3D (coverflow). Audio formats supported: AAC, Protected AAC, MP3, MP3 VBR, Audible.
- Auriculares





NOKIA
Connecting People

NOKIA N95

- Dimensiones: Peso: 120 g / 99 mm x 53 mm / Grosor (máx.): 21 mm.
- Capacidad: Memoria dinámica interna de 160 MB para mensajes, tonos de llamada, imágenes, secuencias de video, notas de la agenda, lista de tareas y aplicaciones. / Ranura para tarjeta de memoria que admite tarjetas de memoria microSD de hasta 2 GB.
- Display: Gran pantalla TFT QVGA (240 x 320 píxeles) de 2,6" con detector de luz ambiental.
- Sistema operativo: Software S60 en sistema operativo Symbian / Teclas multimedia dedicadas / Menú multimedia.
- Camara: hasta 5 megapíxeles / Conexión directa con TV compatible mediante el Cable de Conectividad de Video Nokia / Capacidad para videollamada y videos compartidos (servicios de redes WCDMA) / Flash integrado / Micrófono estéreo digital / Modos de flash: activado, desactivado, automático, reducción de ojos rojos / Blog online: envío de fotos.
- Video: Cámara de hasta 5 megapíxeles. / Conexión directa con TV compatible. / Flash integrado.
- Bateria: Nokia (BL-5F) 950 mAH / Tiempo en conversación: hasta 160 min. (WCDMA), hasta 240 min. (GSM) / Tiempo en espera: hasta 200 horas (WCDMA), hasta 225 horas (GSM).
- Funciones: e-mail / telefonía móvil / mensajería de texto / navegador web nokia con mini mapa.
- MP3: Reproductor de música digital: admite MP3 / AAC / AAC+ / eAAC+ / WMA / M4A con listas de reproducción y ecualizador / Compatible con OMA DRM 2.0 y WMDRM para música / Radio FM estéreo.









MOTO Q

- Dimensiones: Peso: 115 g. / Dimensiones: 116 x 64 x 11,5mm.
- Capacidad: Tarjetas opcionales mini SD™ removibles, para almacenamiento expandible de documentos, fotos, música y vídeo de hasta 1GB.
- Cámara: integrada con 1.3 mega píxel / Windows Media Player Mobile / Grabación y reproducción de video hasta 15 frames por segundo.
- Bateria: Tiempo de conversación estándar de la batería: aproximadamente de 234 minutos. / Tiempo estándar de la batería en espera: aproximadamente de 212 horas. / Tiempo de extendido conversación de la batería: aproximadamente de 339 minutos. / Tiempo extendido de la batería en espera: aproximadamente 311 horas. / Bandas: CDMA-EVDO, Dual Band 800 & 1900 MHz.
- Funciones: Ver e-mails y anexos (documentos, plantillas, presentaciones y PDF's) / SMS / MSN Messenger /Altavoces dobles estereofónicos / Compatible con los formatos más populares de audio y vídeo / Tarjetas opcionales miniSD removOibles, para almacenamiento expandible de documentos, fotos, música y vídeo de hasta 1GB. / Memoria interna de hasta 40Mb. / Enviar fotos, clips de video, texto y audio por e-mail. / Navegar en Internet con Pocket Internet Explorer Mobile.







PALM TREO 750

- Dimensiones: 111 mm x 58 mm x 22 mm / 154 g
- Capacidad: Memoria flash no volátil de 128 MB o 60 MB a disposición del usuario / Procesador Samsung a 300 MHz / Ranura para tarjetas miniSD.
- Sistema Operativo: Windows Mobile 5.0.
- Cámara: 1,3 megapíxeles / Equilibrado de luz automático / Espejo para autorretratos integrado / Compatibilidad con captura de video.
- Batería: extraíble de iones de litio de 1200 mAH. / Tiempo de conversación: hasta 4,5 horas en GSM. / Tiempo en espera: 10 días.
- Conectividad: Tecnología inalámbrica Bluetooth 1.2, infrarrojos (IR) / Compatibilidad con auriculares estéreo.
- Audio: Tonos polifónicos MIDI, MP3, WAV y de video.
- Funciones: Toma de auriculares de manos libres / Opción de silencio del micrófono / Compatibilidad con teletipos TTY/TDD. Posibilidad de personalizar el teléfono añadiendo aplicaciones de software opcionales y accesorios de hardware / Hablar con el kit manos libres gracias a los auriculares estéreo Bluetooth compatibles o utiliza un kit de navegación GPS.









SAMSUNG I600

- Dimensiones: 105 g / 113 x 59 x 11,8 mm.
- Capacidad: 128 MB de ROM y 64 MB de RAM / Memoria externa (micro SD).
- Sistema Operativo: UMTS/ HSDPA / Tribanda (900 / 1.800 / 1.900 MHz) / Windows Mobile 5.0 / WAP 2.0 / La tasa específica de absorción (SAR) más alta para este modelo fue de 0,569 W / kg.
- Camara: 1,3 megapíxeles / Zoom digital (x2) / Autoenfoque / Efectos fotográficos / marcos / Autorretrato / temporizador de disparo / automático / tomas múltiples / Ajustes de calidad fotográfica y tamaño.
- Vídeo: Reproductor de video (H.263, H.264, MPEG4, WMV) / Grabador de video (MPEG 4) / Reproductor de Windows Media 5.0.
- Funciones: Mensajes SMS / MMS / Entrada predictiva de texto T9 / vCard / vCalendar / Envío de e-mails: MS Direct Push / Visor de documentos / Impresión móvil (Bluetooth / USB / Teclado QWERT / Botón rotatorio / MS Outlook / Bluetooth 2.0 / Active SyncML / Outlook Sync / Navegador HTML para Internet / Altavoz / Números marcados / llamadas perdidas / llamadas recibidas / Desvío de llamadas / exclusión de llamadas / llamadas en espera / CLIP / CLIR / Llamadas en grupo / Costo de las llamadas.





BlackBerry





BlackBerry Curve 8300

- DIMENSIONES: Tamaño: 10,7 cm. / Peso: 111,40 grs.
- CAPACIDAD: 64 MB memoria flash / Slot para tarjetas microSD (TransFlash).
- CÁMARA: Cámara digital integrada. 2 mpx. Zoom digital 5x. Flash incorporado. / 64 MB de memoria interna.
- VIDEO: Reproduce Video. / Mensajería Multimedia.
- BATERIA: Bateria de Li-Ion 1000 de alta duración.
- FUNCIONES: Multibanda: GSM/GPRS/EDGE 850 / 900 / 1800 / 1900. / Agenda para múltiples contactos. / Calculadora y Calendario. / Reloj Alarma y Juegos. / Pantalla de 65.536 colores. Función de chat. / E-mail push. / JAVA. / Trasmisión de datos por GPRS, CSD y EDGE. / Conectividad por cable. / Bluetooth. / Compatible con BlackBerry Enterprise Server para Microsoft Exchange / Compatible con BlackBerry Enterprise Server para IBM Lotus Domino / Compatible con BlackBerry Enterprise Server para Novell GroupWise 5 / Integra sus actuales cuentas de correo electrónico profesionales y personales / De forma opcional, integra una nueva cuenta del dispositivo / Incluye software para el equipo de escritorio.
- MP3: reproductor mp3 / Formatos de audio compatibles: MP3, MIDI, AMR-NB, AAC/AAC+/eAAC+, WMA / Formatos de video compatibles: MPEG4 Part 2 Simple Profile, H.263, WMV.





¿Alguien hackeará mi iPhone?



Innovador. Único. Elegante. Con tecnología de punta. Estos son algunos de los adjetivos con lo que lo calificaron. Hasta la revista Times lo consideró el producto del año. Efectivamente estamos hablando del iPhone de Apple, el cual fue sumamente esperado e inmediatamente adoptado por usuarios y fanáticos. Sin embargo, muy poco se dijo acerca de la seguridad de este nuevo dispositivo y pronto se sembró la duda: ¿Alguien podrá hackear mi iPhone?

Y la respuesta no tardó en llegar. Al mes de haber salido al mercado y de haber vendido miles de dispositivos en cuestión de horas, la Independent Security Evaluators (ISE), una investigadora de seguridad de Baltimore fundada por el profesor Avi Rubin de la Johns Hopkins University, dio cuenta de varias vulnerabilidades que afectaban directamente al dispositivo de Apple y que ponía en jaque a toda su seguridad y a la información que los usuarios mantenían en él.

La más importante encontrada por los investigadores Charles Miller, Jake Honoroff y Joshua Mason fue la del sistema operativo del teléfono, el Mac OS X y el navegador Safari 3.03 en versión beta.

El peligro de este agujero residía en que los usuarios, al visitar una página Web maliciosa se les descargaba un exploit a través del cual el criminal podía tener acceso a los mensajes SMS, a la libreta de direcciones, al historial de llamadas y al buzón de voz. Es decir que tenía acceso a información sensible guardada en el dispositivo.

Según informó Apple, para instalar los parches y estar resguardados de posibles ataques, los usuarios del iPhone necesitaban de conexión a Internet y de la última versión de iTunes. De esta forma, al conectarse al iTunes, automáticamente aparece la notificación de actualización. Si bien la empresa de Steve Jobs recomienda fuertemente instalar todos los parches, aquellos que deciden no hacerlo volverán a tener la posibilidad una vez que se vuelvan a conectar.

De todas formas, la aparición de esta vulnerabilidad le abrió los ojos a los usuarios y principalmente a la empresa. Pero no todo se quedó ahí.

El debate comenzó

Apenas Google anunció el lanzamiento de una plataforma abierta para teléfonos móviles de nombre Adroid el debate acerca de las plataformas basadas en Linux y su seguridad no tardó en comenzar.

El debate acerca de la relativa seguridad del open source respecto de los software propietarios es bastante vieja. El desarrollo del software open source cuenta con la ventaja de tener varios pares de ojos revisando el código, en busca de notorias irregularidades, por lo que los parches que tapan dichas vulnerabilidades pueden ser escritos y lanzados rápidamente. Sin embargo, una de las desventajas es que cualquiera puede examinar el código en busca de vulnerabilidades y escribir exploits.

Por otra parte, el código fuente del software propietario no puede ser visto directamente, por lo que las vulnerabilidades solo podrán ser encontradas a través de ingeniería inversa. Sin embargo, como poca gente puede acceder a este código fuente es probable que sea un software con muchos fallos o bugs. Algunos expertos, además, enfatizan que una vez que una vulnerabilidad es encontrada, el lanzamiento de las actualizaciones es muy lento, especialmente con las compañías multinacionales de software.

Muchos de los vendors de seguridad tratan de evitar tomar posición afirmando que es como comparar peras con naranjas. Jan Volzke, global marketing manager de McAfee Mobile Security, afirmó que no es posible comparar la seguridad de los dispositivos basados en Android y los del iPhone de Apple. “El iPhone de Apple no tiene nada que ver con el open soruce. En cambio Apple brindará un kit de desarrollo”, afirmó Volzke. “La comparación entre los desafíos de la seguridad de una plataforma de un dispositivo open source versus un kit de desarrollo de software de un dispositivo específico tendrá diferentes conclusiones”.

Un vendor de seguridad estuvo dispuesto a realizar una predicción



La seguridad de los nuevos dispositivos celulares es un tema que preocupa a más de uno y abre el debate: ¿plataformas abiertas o software propietarios?

pero con cautela. Ben Whitaker, jefe de seguridad de la empresa Masabi de desarrollo de seguridad móvil, se inclinó con cautela para el lado del open source. “Gphone es open source, lo que significa que es un muy buen comienzo y puede ser trabajado casi por cualquiera”, afirmó Whitaker. “Empezó de una mejor manera que el iPhone, al cual ya se le han encontrado vulnerabilidades. Sin embargo, ningún nuevo consumidor (tanto del iPhone como del Gphone) estará seguro apenas se lanza el producto”.

Whitaker afirmó que dada la cantidad de vulnerabilidades del iPhone, la conectividad de Internet de este smartphone será mucho más vulnerable que la de un móvil con una plataforma Java, la cual fue clasificada como semi inteligente.

En el caso del iPhone, “con cualquier nuevo navegador, los sitios web maliciosos tomarán ventaja de las vulnerabilidades de Ajax, JavaScript y ActiveX”, dijo Whitaker. “Un móvil menos inteligente es también menos vulnerable. Los desarrolladores de Android se tendrán que mantener a una plataforma de semi smartphone porque la Java sandbox brinda protección contra los ataques más comúnes”.

Whitaker agregó que, como el iPhone, el dispositivo de Google tendrá vulnerabilidades. “El Gphone brindará la posibilidad de correr aplicaciones sobre él, las cuales podrán estar abiertas a los keyloggers”, sentenció Whitaker. “Hasta el momento, la plataforma de Gphone no corre sobre un archivo del sistema encriptado y tiene un log-in vulnerable”.

Con mucho trabajo de desarrollo por realizar, los expertos aún no tienen una posición tomada. Pero una cosa sí es segura: ningún dispositivo que se conecte con el exterior puede ser totalmente seguro, y ni el iPhone ni el Gphone serán la excepción.

Pablo Eduardo Hernández
Ingeniero en sistema de la información



Cómo sobrevivir a una contingencia y no morir en el intento

FOTO: http://www.sxc.hu/ - Manoj M

Preparando la hoguera

Lamentablemente las empresas en el mundo no empiezan sus negocios pensando que algún día puede ocurrir una catástrofe, tanto en la fase de implementación como así también en la etapa de producción; por el contrario terminan la implementación y se dan cuenta de que si llegase a ocurrir un incidente se generaría una pérdida de ingresos monetarios y, por supuesto, que además podrían dejar de dar servicio a áreas claves de la organización como logística, administración, recursos humanos, etc...

Muchas veces, incluso, no se tiene en cuenta que la pérdida no es solo material, sino que también pierden en lo que respecta a la imagen corporativa, a la percepción de la empresa por parte de los clientes o proveedores, en los beneficios que una interrupción en el servicio puede darle a la competencia para obtener ventajas competitivas.

Que una organización se prepare para una contingencia, no significa que reconozca la ineficacia de sus procesos, sino que supone un avance a la hora de superar cualquier eventualidad que pueda acarrear perdidas y llegado el caso no solo materiales sino hasta humanas.

La necesidad de las organizaciones actuales, cada vez más dependientes de la tecnología, demanda una conciencia activa por parte del CIO y la alta gerencia para poder anticiparse a las contingencias antes que éstas acaben con la empresa.

Encendiendo el fuego

Si bien está claro que el objetivo de toda organización es poder continuar trabajando a pesar de una catástrofe, suena alienante a los oídos de alguien que alguna vez ha visto los efectos de un huracán (al menos por televisión o en una fotografía), o los actos de vandalismo de alguna corrida popular, o incluso un incendio, pensar que la propia organización está exenta a cualquier problema; algo así como que contase con una protección divina que inhibe cualquier fuerza humana o natural que les quiera perpetrar daño: el que piensa así se expone a consecuencias que pueden llegar a ser irreparables para la continuidad de la empresa si esa "protección divina" llegara a fallar.

Para seguir avanzando vamos a definir lo que es una **contingencia:** ***"Es una interrupción en los procesos críticos del negocio, que tiene las siguientes características:***
• No está planificada
• Puede perdurar indefinidamente en el tiempo.
• La misma no está contemplada por las normas y los procedimientos de la empresa".

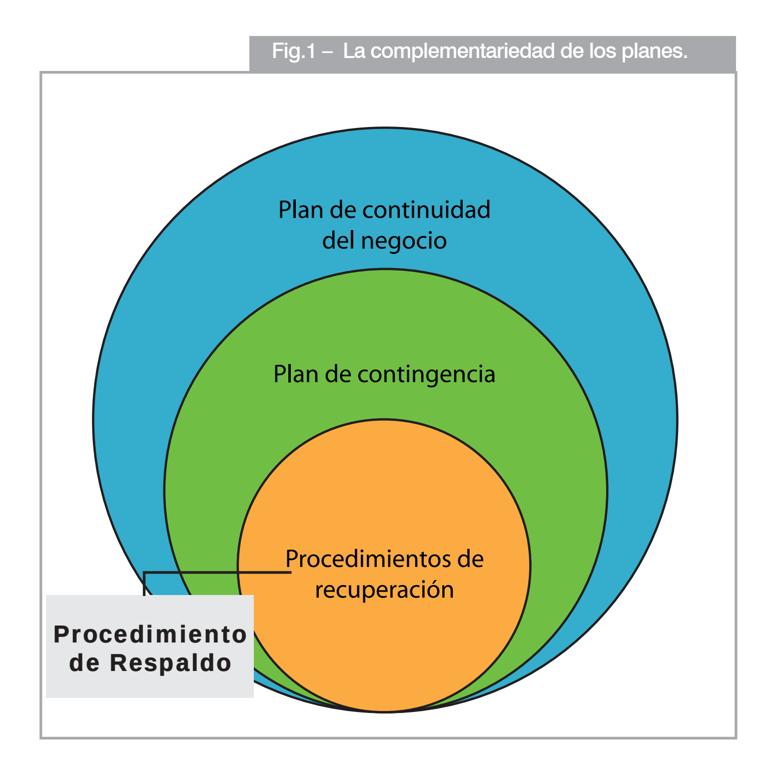
Vamos a explicar un poco todo esto con un ejemplo para aclararlo: si se inicia un incendio en el centro de cómputos, va a producir indefectiblemente la interrupción de uno o más procesos críticos del negocio, ya que como mencioné antes, los mismos son cada vez más fuertemente dependientes de la tecnología. Esta interrupción por cierto que no estaba planificada: es decir nadie decidió cuándo se iba a producir el fuego. Seguramente en algunas horas posteriores al incendio los bomberos habrán de apagarlo, pero ciertamente que no podemos saber cuándo volveremos a dar servicio, y por último esta interrupción no va a estar en ningún manual de procedimientos, esto quiere decir ningún manual de procedimientos va a decir algo así como "Una vez al mes encender un fuego en el centro de cómputos...", aclaro esto dado que en realidad sí vamos a saber qué hacer en caso de un incendio, pero en ese momento la interrupción ya ocurrió y solo algún "plan" nos ayudará a volver a tener todas las funciones criticas operativas nuevamente.

Cuando todo está ardiendo

Llegó el momento de poner toda la carne al asador: voy a intentar explicar un poco, en forma resumida ya que es algo muy amplio y no hay una convención en cuanto al nombre estricto, qué es esto de los distintos tipos de "planes" y cómo cada uno es complementario del otro; lo podemos imaginar como las capas de una cebolla. En la figura 1 se puede ver mejor el concepto.

En el centro de la cebolla están los "Procedimientos de recuperación" (o procedimientos operacionales) que son los que detallan la recuperación de un proceso de negocio especifico, que puede estar informatizado o no. Este procedimiento se encargará de describir uno a uno los pasos necesarios para recuperar exitosamente dicho proceso, y también incluirá si fuera necesario la descripción de los recursos humanos y materiales para una eficiente recuperación.

Fig.1 – La complementariedad de los planes.



Podemos ver que el centro de la cebolla se relaciona directamente con los "Procedimientos de respaldo", y estos son los mejores amigos de los CIO que tengan procesos de negocio informatizados, ya que si no hay un buen respaldo de los servidores que soportan esas funciones es poco probable que las mismas vuelvan a quedar operativas.

La capa del medio de la cebolla hace referencia al "Plan de contingencia" (o también llamado DRP – Disaster Recovery Plan), este plan que incluye uno o muchos procedimientos de recuperación, es más funcional que el anterior, contempla todos los pasos que deben ser realizados desde que se detecta una contingencia hasta que la empresa queda totalmente operativa en el sitio alternativo. El sitio alternativo no es ni más ni menos que lo que se deduce de su nombre, en caso de un desastre en la propia empresa los empleados tendrán que seguir trabajando en otro lugar físico con todas las comodidades necesarias para poder seguir ejerciendo su función. Este plan está acotado solo al área de sistemas, específicamente a un desastre en el centro de cómputos.

En caso de contingencia las perdidas no son solo materiales, también involucran pérdidas de imagen, de percepción frente a los clientes y pérdida de terreno ante la competencia; llegando en el peor de los casos a ocasionar pérdidas humanas.

FOTO: http://www.sxc.hu/ - Rodolfo Clix - April Milam

Por eso la capa superior habla del "Plan de continuidad del negocio" (o BCP – Business Continuity Plan), este plan que incluye un DRP, y uno o varios procedimientos de recuperación por áreas, es el más funcional de todos los aquí presentados, y no se refiere solo al área de sistemas, sino que involucra a todas las áreas de la organización.

Después del incendio, solo queda humo

Hasta acá hablamos de la necesidad de contar con un plan para estar preparados para cuando aparezca un incidente, pero lamentablemente con esto solo no alcanza, hay que al menos tener en cuenta estas otras tres consideraciones adicionales:

1. Actualizar el plan. Cada cierto periodo de tiempo la empresa tiene la obligación de auto revisar el plan y ver si su contenido aún sigue siendo vigente.
2. Realizar, al menos, una prueba del plan anualmente. Es la única forma de saber si todos los componentes del plan son correctos, y si realmente nuestro plan cumple con el objetivo de recuperar los procesos críticos del negocio.
3. Realizar periódicamente una auditoria externa del plan (no confundir con actualización) para descubrir falencias en el mismo.

El alma del fuego

Nuestro plan de continuidad se basa en premisas previamente acordadas y las mismas responden a la necesidad de la empresa de mantenerse operativa. Es así que existe algo que se llama ventana de indisponibilidad que va de la mano con la estrategia de recuperación. Hay entonces un estrecho vínculo costo/beneficio implícito en esto que acabo de mencionar, es decir cuanto más rápido tenemos que volver a estar productivos más cara será para nosotros la estrategia de recuperación que nos permita esto.

Como se puede ver en la figura 2 – Relación costo/beneficio en la elección de la estrategia de recuperación, el costo por la interrupción del servicio aumenta en función del tiempo, es decir cuanto más tiempo estemos sin servicios, más caro le saldrá a la empresa. Esto es así porque una empresa en contingencia puede dejar por ejemplo de facturar y procesar los pagos que le realicen sus clientes, razón por la cual los ingresos pueden llegar a ser nulos, pero por otro lado los proveedores que no se encuentran en contingencia seguirán facturándole los servicios prestados/contratados.

Por otro lado, el costo de recuperar tiende a ser menor a medida que pasa el tiempo, esto se debe a que si queremos una recuperación de "tiempo 0" tenemos que tener armado un esquema en donde todos nuestro procesos críticos informatizados estén replicados en un sitio remoto, y por supuesto que esto impacta en el costo de la recuperación.

En mi experiencia el 80 por ciento de las empresas hacen respaldos de información incorrectos, porque ponen foco en resguardar los datos de usuario, y no piensan que ese servidor eventualmente tendrá que ser recuperado en un sitio alternativo y posiblemente en un hardware distinto al que se utilizaba cuando aún estaba en producción.

El equilibrio se produce entonces en donde las 2 líneas se cruzan, que es donde se balancea el costo de recuperación con el costo de no operar. Para obtener este balance hay algunos análisis que se pueden realizar, entre ellos un BIA (Business Impact Analysis) cuyo objetivo es relacionar las funciones criticas del negocio con la tecnología utilizada, y basado en esa información, caracterizar las consecuencias de una interrupción del sistema.

En este punto entonces podemos concluir que sabemos claramente cuánto tiempo podemos estar sin brindar servicios, y algo que está estrechamente ligado a esto: desde cuándo necesitamos tener la información disponible para lograr una recuperación exitosa: esto es entonces lo que se conoce como RPO (Recovery Point Objetive) y RTO (Recovery Time Objetive) como se ve en la figura 3.

El punto de recuperación (RPO) tiene que ver con algo crucial en una contingencia, y es saber ¿Cuál es el último respaldo de datos disponible con el que cuenta la empresa? Cuanto más antiguo sea éste más información la empresa perderá (o tendrá que reprocesar). El segundo, el tiempo de recuperación (RTP) o ventana de indisponibilidad, habla de cuánto tiempo puede estar la empresa "parada". Como se ve claramente en el gráfico ambas cuestiones tienen estrecha relación con la estrategia elegida, y como dije anteriormente, eso es la relación costo/beneficio que es particular en cada caso.

Fig.2 – Relación costo/beneficio en la elección de la estrategia de recuperación

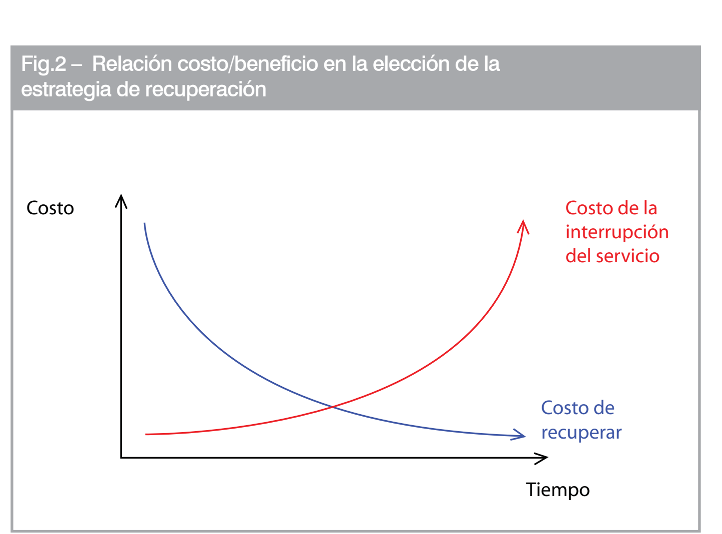


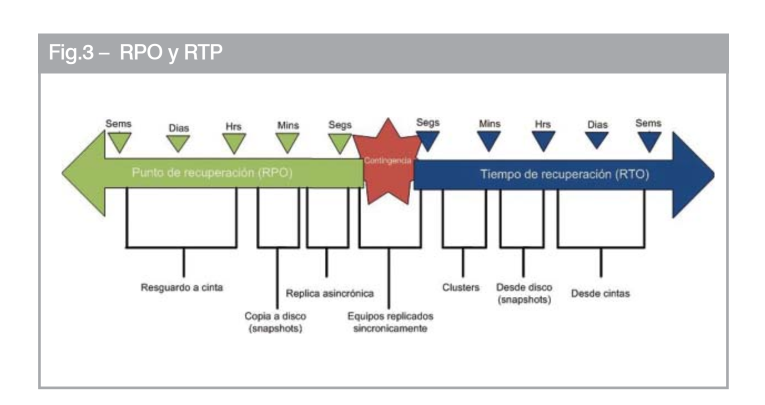
FOTO: http://www.sxc.hu/ - Rodolfo Clix - patryk specjal - Matt Dragseth - Matt Dragseth

Recolectando maderitas antes de prender el fósforo

En esta materia si bien existe mucho material "circulando" por Internet, poco del mismo encara al tema con la seriedad que se merece, y además en la Argentina existen pocos profesionales dedicados y capacitados para llevar adelante proyectos coherentes en materia de la relación desastre - recuperación, que es donde debería empezar cualquier proyecto de este tipo.

Yo sugiero a los CIO (o a la alta gerencia) que comenzar por asegurarse que exista una política de resguardo apropiada es la base indispensable para tener éxito en la aplicación de cualquier procedimiento definido para la continuidad del negocio. ●

Fig.3 – RPO y RTP



Información Profesional



Pablo Eduardo Hernández es Ingeniero en sistema de la información con un Post-Grado en Seguridad informática y auditoria de sistemas. Como experiencia profesional tiene más de 5 años asesorando empresas en el área de BusinessContinuity Services.

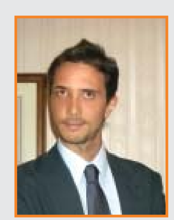
Lectura complementaria

National Institute of Standars and Technology: http://www.nist.gov
IRAM: www.iram.com.ar
Norma ISO 27001: http://www.iso27000.es/

Notas de la Serie

#1: Contingencia.
#2: BIA, Business Impact Analysis .
#3: DRP, Disaster Recovery Plan.
#4: Procedimientos de respaldo.

Windows Server 2008: Pila Next Generation TCP/IP



Martín Sturm
Regional Project Manager
Aon Risk Services
Latin America

Si bien ya se encuentra incluida en la última versión del sistema operativo Windows para clientes (Microsoft Windows Vista), la nueva implementación de la suite del protocolo TCP/IP conocida como la "Pila Next Generation TCP/IP" será también incorporada en el futuro Sistema Operativo para Servidores Windows Server 2008 (Hoy en Beta 3 o RC0).

La pila del protocolo TCP/IP fue originalmente diseñada en los 90 y con el tiempo mejorada para encontrar las necesidades de los usuarios hogareños y empresas.
Lo cierto es que ya la pila existente en Microsoft Windows 2000 introducía un set de mejoras de performance, que incluían: TCP Receive Window Scaling, Acknowledgments Selectivos, y Mejor estimación de roundtrip time (RTT), pero a lo largo de los años a esta versión de Windows y tras la sucesión de grandes cambios a nivel infraestructura, diferentes modificaciones sobre lo existente se fueron sumando para lograr importantes mejoras de performance.
A diferencia de esto último, la nueva Pila Next Generation TCP/IP tanto en Windows Vista como en Windows Server 2008 (por el momento en testing) es un rediseño total de la funcionalidad de TCP/IP para ambas versiones del protocolo de Internet: IPv4 e IPv6, que encuentran las necesidades de conectividad y performance de los variados entornos y tecnologías de hoy en día, incluyendo un nuevo set de mejoras de performance para incrementar el rendimiento del procesamiento en anchos de banda altos, alta latencia y entornos de red con alta pérdida.

De las mejoras comprendidas, se detallan las más significativas:
• Receive window auto-tuning
• Compound TCP
• ECN Support
• Enhancements for high-loss environments
• TCP Fast Reconnect
• Improved routing path detection and recovery

Esta nueva pila presenta características que la convierten sin dudas en la nueva generación TCP/IP, enumerando algunas de ellas tendremos:

Arquitectura de doble capa de IP para IPv6

La pila Next Generation TCP/IP tiene habilitadas IPv4 e IPv6 de manera predeterminada por lo que no es necesario instalar ningún componente adicional para obtener compatibilidad con IPv6.
Es importante recordar que la implementación de IPv6 en Windows XP y Windows Server 2003 es una arquitectura de doble pila. Esto es que para disponer de compatibilidad con IPv6 es necesario instalar un protocolo adicional a través de la carpeta Conexiones de red. Esta pila adicional del protocolo IPv6 incluye su propia capa de Transporte la cual a su vez comprende por un lado el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP) y por el otro su propia capa de Tramas, por lo que todos los cambios a los protocolos tanto en esta última capa como en la de Transporte se deben realizar en dos controladores de Windows: Tcpip.sys para la pila del protocolo IPv4 y Tcpip6.sys para la pila del protocolo IPv6.
Precisamente, la pila Next Generation TCP/IP al ser compatible con la arquitectura de doble capa IP en la que las implementaciones de IPv4 e IPv6 permite que ambas, Transporte y Tramas sean completamente compartidas.

Extensibilidad nueva

Con su nueva infraestructura, esta nueva pila permite que más componentes se puedan insertar y quitar de manera modular y de forma puramente dinámica.

Compartimientos de enrutamiento

Esta nueva pila Next Generation TCP/IP es compatible con compartimientos de enrutamiento, con lo que es posible evitar el trafico no deseado entre las interfaces de una VPN, de Terminal Server o inicios de sesión de usuarios múltiples.
Conceptualmente se lo conoce como compartimiento de enrutamiento a la conjunción de interfaces con un inicio de sesión con tablas de ruteo propias.
En la práctica y como ejemplo, si iniciamos, vía Internet, una sesión de VPN utilizando la pila TCP/IP existente hoy en día, tendremos acceso no solo a la VPN en sí misma, sino también a Internet a través del uso de registros en la tabla de enrutamiento de IPv4 mediante la Intranet privada previamente creada. Como ventaja, los compartimientos de enrutamiento de la nueva pila Next Generation TCP/IP permiten aislar la conectividad de Internet de la conectividad de la Intranet privada ya que administra tablas de enrutamiento IP independientes.

Nueva API y Seguridad para el filtrado de paquetes

Un nuevo Framework conocido como Windows Filtering Platform (WFP) nace para reemplazar una serie de viejos componentes como el almacenamiento de la información de filtros de paquetes existentes en la pila actual.
Este Framework es mucho más seguro ya que se encuentra fuertemente integrando en la pila, y resultando más simple para que los proveedores independientes (ISV) puedan crear drivers, servicios y aplicaciones para filtrar, Inspeccionar y modificar el tráfico TCP/IP.

Configuración automática en base al descubrimiento del entorno de red disponible

Al identificar el entorno de red existente, nos ajusta los valores más importantes de la configuración de red (como por ejemplo la ventana de recepción de TCP) para lograr un óptimo rendimiento. Se logra una mejora en la administración de la configuración de TCP/IP y se aumenta la productividad al simplificar tareas administrativas de IT.

Simplificación en la programación de red en modo kernel

Aparece una nueva compatibilidad, precisamente con el núcleo Winsock (WSK), básicamente se trata de una nueva interfaz de programación en modo kernel diseñada para sustituir a la interfaz de controlador de transporte (TDI) en Windows XP y Windows Server 2003.



No más reinicios de equipo tras los cambios de configuración

Al utilizar un nuevo método para el almacenamiento de la información de la configuración, la pila Next Generation TCP/IP tiene un control mucho más dinámico, lo que deriva en la no necesidad del reinicio de los equipos después de una modificación.

Nueva compatibilidad para el escalamiento en equipos con más de un procesador

Es sabido que una limitante en las arquitecturas hasta la versión NDIS 5.1 no permite procesar protocolos en más de un procesador, lo que se presenta como problemático a la hora de manejar volúmenes de tráfico de red significativos. Por ello, el concepto de receive-side scaling o escalación del lado del receptor, incorporado en la nueva pila, permite en principio resolver este tipo de problemas permitiendo que la carga de la red de un adaptador sea equilibrada entre más de un procesador.

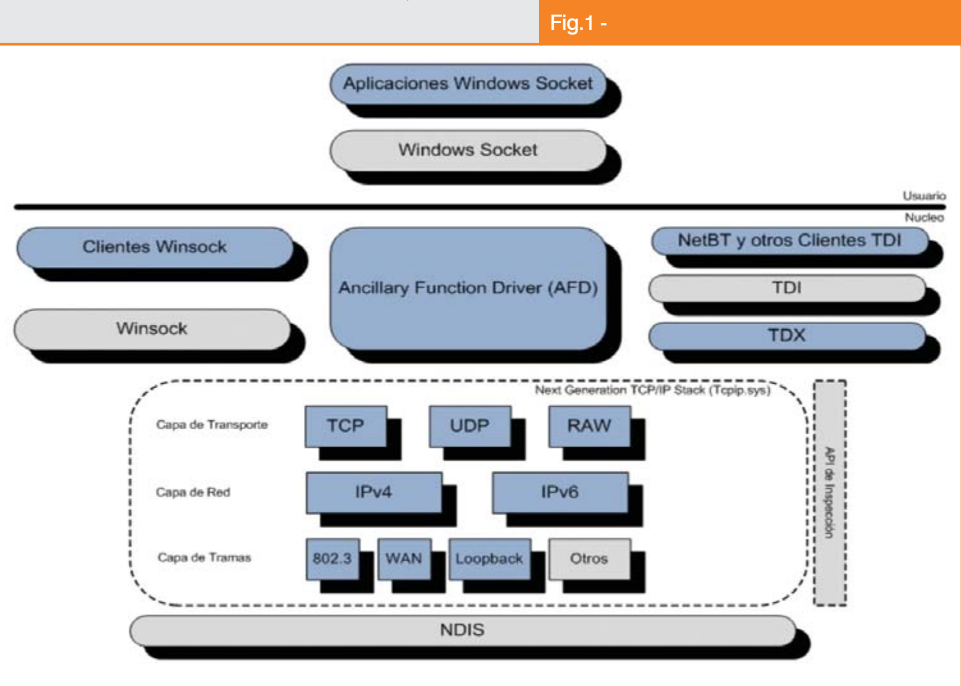
Arquitectura de la pila Next Generation TCP/IP

La siguiente imagen muestra la arquitectura de la pila Next Generation TCP/IP.
Como se puede apreciar en la misma, existen tres APIs principales por donde los servicios y aplicaciones acceden a la pila Next Generation:
1.WSK: Que es utilizada por los clientes de Winsock.
2.Windows Sockets: Esta API trabaja a través un driver llamado Ancillary Function Driver (AFD) para lograr funciones de socket con TCP/IP y es utilizada por los servicios y aplicaciones basadas en Windows Sockets.
3.TDI: Que es utilizada por NetBIOS sobre TCP/IP (NetBT) y aquellos clientes TDI heredados. Por su lado, TDX es una capa que permite la conversión entre la nueva pila y TDI.
Adicionalmente, se observa una API Inspection comprendida dentro del WPF, la cual realiza una inspección avanzada, con posible modificación sobre el contenido de los datos de los paquetes.
Es interesante remarcar que la Pila Next Generation esta compuesta por las capas de Transporte, Red y Tramas, ofreciendo acceso a las rutas de procesamiento de paquetes tanto en la capa de Red como en la de Transporte y enviando y recibiendo tramas a través de NDIS.

En síntesis

Si bien es posible enumerar características y/o mejoras de la pila Next Generation TCP/IP, puede que resulte difícil que estas sean percibidas por el usuario final, incluso en determinados casos por el mismo administrador de IT.
En cambio y sobretodo en la práctica, se estima que si se podrá experimentar y percibir claras mejoras en el rendimiento de TCP para redes de alta velocidad, redes inalámbricas y demás redes de gran pérdida, sumado a esto, la resistencia mejorada frente a todos los ataques conocidos de denegación de servicio. ●

Fig.1 -



EL NEGOCIO QUE GANA LA CREDIBILIDAD



En nuestro issue anterior publicamos un análisis acerca de Google como empresa, su política de información y de privacidad, su política de recursos humanos y qué es lo que muchos de sus empleados y ex empleados opinaban al respecto.

En este caso NEX IT entrevistó a Alberto Arebalos, Director de Corporate Communications & Public Affairs para Latinoamérica de Google quien nos dio su punto de vista.

INTELIGENCIA DE NEGOCIOS AL ALCANCE DE TODOS

crystal xcelsius

Realiza tableros de control interactivos y presentaciones de negocio con cualquier tipo de datos.
Integra los tableros y presentaciones con documentos Microsoft Office, presentaciones Flash y PDF y los comparte a través de la web.
Presenta la información de forma interactiva, con una excelente calidad visual.
Permite crear presentaciones de datos a partir de Excel y web services.

crystal reports

Software Líder en elaboración de informes. Los usuarios generan reportes avanzados en forma intuitiva y fácil.
Herramienta para diseño e integración de informes, para las plataformas de desarrollo más difundidas, integrando datos en forma dinámica en aplicaciones Web y Windows (.NET, Java, PHP, Eclipse, etc.).
Permite diseñar informes con recursos provenientes de cualquier fuente de datos e integrarlos en portales (Websphere, Sharepoint, etc.)







VISITE WWW.ZONA-CRYSTAL.COM Ó LLÁMENOS AL 5217-1227/8/9

NEX IT: ¿Qué le diría a quienes afirman que el crecimiento de Google como compañía es gracias a la utilización de la información de sus usuarios en su propio beneficio?

Alberto Arébalos: Me cuesta mucho responder esta pregunta porque no existe una relación de causa y efecto. Es decir, creo que hay mucho de ficción en este pensamiento porque desde Google no tenemos forma de saber lo que la gente quiere.

Google como buscador es exitoso porque los resultados que brinda son relevantes a las búsquedas realizadas. Hasta los links sponsoreados son relevantes, no permitimos que cualquier link surja como resultado.

Lo que sí podemos determinar es la IP desde donde se realizó la búsqueda y en qué consistió esa búsqueda, pero no asociarlo con una persona determinada. Es decir, nosotros sabemos que por ejemplo en Argentina la palabra más buscada fue tal o cual, pero estas búsquedas no se asocian a una persona en particular ni se conoce su situación y además porque las IP son anónimas, sin contar que se pueden realizar búsquedas desde celulares, laptops, etc.

NEX IT: ¿Cuál es la política de privacidad de Google?

A.A: Nuestra política está regida por un lado por las leyes y por el otro por los principios propios.

Es decir, Google cumple con los procesos legales válidos, como órdenes de registro, órdenes judiciales o mandamientos solicitando información personal. Estos mismos procesos se aplican por todas las compañías respetuosas de las leyes. Como siempre ha sucedido, las primeras protecciones que tiene contra las intrusiones por parte del gobierno son las leyes aplicables en el lugar donde resida.

Además, Google cumple con los principios del puerto seguro sobre la protección de la vida privada de los Estados Unidos de Notificación, Elección, Transferencia Ulterior, Seguridad, Integridad de la Información, Acceso y Aplicación, y está registrado en el Programa Puerto Seguro ("Safe Harbor Program") del Departamento de Comercio de Estados Unidos.

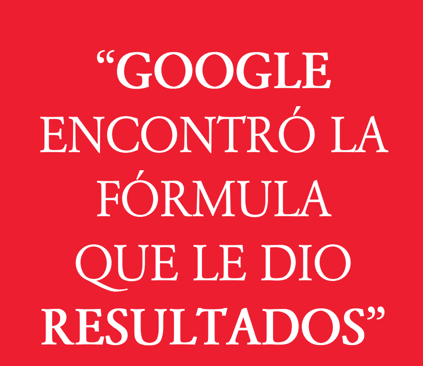
De todas formas nosotros hacemos pública nuestra política de privacidad y cada vez que un usuario quiere registrarse a un servicio nuestro deberá pasar por esa instancia.

NEX IT: Muchos usuarios tienen fotos, blogs, videos, calendario, e-mails, feeds de noticias, mapas, contactos, documentos, hojas de cálculos, presentaciones y hasta información de su tarjeta de crédito subida al servidor de Google. ¿Cómo manejan la seguridad de esta información? ¿No es peligroso que una sola compañía tenga toda esta información de un usuario?

A.A: La información de cada aplicación está alojada en servidores separados, por lo que es bastante irreal pensar que en un solo lugar se tiene todo lo necesario como para conocer al que está del otro lado.

Más allá de este miedo existe una realidad: la credibilidad es nuestro negocio, por lo que atacarla o ponerla en riesgo es algo que evidentemente no nos beneficia. No tiene ningún sentido, aunque hay mucha gente que adora las teorías conspirativas...

De todas formas es ilógico ir en contra de nuestros propios intereses porque en definitiva Google es un negocio.



"GOOGLE ENCONTRÓ LA FÓRMULA QUE LE DIO RESULTADOS"

NEX IT: ¿Cómo surgió el slogan "Don't be evil"?

A.A: El slogan fue invento de un ingeniero cuando necesitábamos definirnos como empresa. Por lo que empezamos a pensar cómo somos como empresa y cómo nos queríamos comportar como tal. De ahí salieron cosas como portarnos bien, que los empleados estuvieran contentos, etc. En resumen, que no fuéramos malos.

NEX IT: Google incentiva a que sus empleados inviertan el 20 por ciento de su tiempo en proyectos propios. Sin embargo algunos Xooglers afirman que este 20 por ciento se traduce en un total de "120" por ciento de trabajo (es decir, resta un poco a las horas libres) ya que no encuentran el tiempo necesario para cumplir con sus tareas más el plus de innovación. ¿Cree entonces que esta política está bien aplicada?

A.A: La verdad creo que no se puede generalizar. Habría que analizar cada caso en particular porque lo que se incentiva en Google es que cada empleado pueda desarrollar proyectos propios y de esta forma seguir innovando. De este programa surgieron proyectos como el Gmail y el Google Earth.

Además nuestros empleados no cumplen un horario fijo de trabajo por lo que es imposible contabilizar o medir si se trabaja un "120" por ciento.

NEX IT: De acuerdo a los resultados arrojados hasta el momento de su innovadora política laboral (trabajo por objetivos, entretenimiento y dispersión en horario laboral, lavandería, pileta, etc) en el GooglePlex, ¿la recomendaría a las demás empresas?

A. A: Hay algo que es cierto y es que la gente responde mejor a los estímulos positivos que a los negativos.

Voy por partes, nosotros empleamos a gente inteligente y más que nada a gente brillante, por lo que también es un desafío para nosotros encontrar a estos talentos y representa un desafío aún mayor que estén contentos en su ambiente de trabajo.

Sin embargo la política que mantenemos en Google no la podemos recomendar a todas las empresas porque depende de la política de Recursos Humanos de cada compañía en particular.

Google encontró una fórmula que le dio resultados y con la cual los empleados están contentos y rinden al 100 por ciento porque están conformes. ●

Acerca de la elección del tipo de software

La renovación del sitio en el que Microsoft compara Windows con Linux, el análisis que se hace del hecho en medios importantes y la posibilidad de que la realidad sea bastante distinta de la que nos quieren mostrar o hacer creer, no tiene que desviarnos de nuestro verdadero objetivo: resolver el problema de nuestro cliente de la manera más ventajosa para él, no para nuestros proveedores.

Ricardo D. Goldberger
Periodista Científico especializado en Informática y Nuevas Tecnologías

Hace algunas semanas, Mary Jo Foley, la responsable del blog All About Microsoft de ZDNet (1) publicó un artículo señalando que el famoso sitio "Get The Facts", en el que Microsoft trataba de demostrar que Linux resultaba tanto o más caro que Windows, a la hora de implementarlo en servidores o empresas, había sido cerrado y reemplazado por otro llamado Compare (2), en el que básicamente se aseguraba lo mismo, pero complementándolo con algunos artículos comparando otros sistemas operativos (Windows vs. Unix) y otros productos (IIS contra Apache, por ejemplo) y enfocando la artillería más específicamente en Red Hat que en un genérico "Linux".

Microsoft tiene, por supuesto, todo el derecho del mundo, como lo tiene cualquier empresa, ya sea de tecnología como de otro segmento, en generar todas las campañas y utilizar todas las herramientas (fíjense que no dije "armas") legales y legítimas que crea necesarias para promocionar sus productos y demostrar que son mejores que los de la competencia.

A lo que a ninguna empresa asiste, es el derecho de mentir, que es lo que muchos han opinado acerca del famoso Get the facts. Cuando Microsoft plantea que es un mito que Linux sea gratuito y trata de demostrarlo a través de sitios y documentos como estos de los que estamos hablando, la respuesta que recibe desde el ambiente del software libre es "nunca dijimos que Linux sea gratis". El mismo Richard Stallman asegura que el software libre debe ser comercializado como cualquier otro producto, porque el concepto de free significa, para este caso, libre, no gratis.

De la misma manera, cuando se clasifica al combate como "comercial vs. libre", también se está incurriendo en denominaciones prejuiciosas (denominando como tales a las que se hacen desde uno de los lados en perjuicio del otro, tal como, desde "el otro" se llama privativo al software propietario). En rigor, ninguna de las clasificaciones resulta totalmente neutral, porque incluso cuando se menciona que hay modelos que "respetan la propiedad" intelectual, oponiéndolos a los que no lo respetan, y dan como ejemplo al software libre, la realidad es que ambos "sistemas" regulan el uso del producto por parte de su productor, sólo que lo hacen de manera distinta. Por lo tanto, en ambos casos se están protegiendo los derechos del productor, pero desde distintos marcos conceptuales.

Ahora bien, ¿cuál debería ser nuestra posición? ¿Deberíamos dejarnos llevar por las cuestiones "ideológicas" o estamos hablando de negocios? Por supuesto, nadie está exento de actuar desde una perspectiva ideológica, y no sería quien esto escribe uno de los que lo negarían.

Pero cuando se trata de un negocio en el que está en juego la inversión, la productividad y, sobre todo, los resultados, en ocasiones debemos juzgar y concluir en base a conceptos financieros o mercantiles, más que económicos o sociales. En definitiva, cada uno hace la elección con la que se siente más a gusto.

Eso obliga, por supuesto, a cierta apertura mental de la que no todos podemos hacer gala.

Pongamos por caso lo siguiente: un reciente estudio de IDC acerca de los embarques de servidores muestra que, después de un pico del 41% en el año 2004, el porcentaje de servidores con Linux instalado promedia el 12 o el 13% de manera estable en los cuatro últimos trimestres. Para algunos, no significa nada. Para otros, en cambio, es muy probable que Linux haya encontrado su nicho de negocios y ese 12 o 13% será (sería) su espacio más cómodo en los datacenters de las compañías.

De lo que se trata, es de resolver el problema de nuestro cliente. Si es con software libre, con propietario, con una combinación de ambas, es muy probable que la elección final se base en la ecuación inversión/resultado, o precio/prestación o retorno de la inversión, que en si se ha desarrollado de tal o cual manera.

En definitiva, no son los folletos publicitarios ni los estudios de marketing tendenciosos ni la publicidad abierta o encubierta lo que nos debe alejar de nuestro foco: resolver el problema de nuestro cliente de la manera más ventajosa para él, no para nuestros proveedores. ●

(1)http://blogs.zdnet.com/microsoft/?p=670
(2)http://www.microsoft.com/windowsserver/compare/default.mspx

Luis Vinay
Consutor Senior
Xtech

MUCHO SE DICE QUE XEN ES LO QUE SE VIENE PERO MUY POCO REALMENTE SE CUENTA DEL PROPIO XEN.

EL ARTE DE LA VIRTUALIZACIÓN SEGÚN XEN

La versión libre de Xen lleva la virtualización hasta donde quien la use se anime. Utilizando la potencia y flexibilidad de Xen con las ultra conocidas y confiables herramientas de Linux, la infraestructura de virtualización se adapta a usted y no al revés. Redescubramos juntos la potencia de la simpleza.

Unas palabras antes de empezar

En los últimos años, especialmente en este último, la virtualización *"it's getting momentum"* como dicen los angloparlantes o está en pleno auge, y no es casualidad ya que como sabe todo aquél que conoce o posee un *Datacenter*, los beneficios de esta técnica de multiplexación de recursos son muchos y muy importantes, no pretendo extenderme demasiado en esto, pero no está de más enumerar algunos de los más importantes:

• *Uso intensivo del hardware*: Con la potencia de los equipos de hoy en día tener un servidor dedicado a un único servicio es seguramente tener capacidad ociosa, y por lo tanto un desperdicio de dinero.

• *Uso intensivo de la infraestructura del datacenter:* Esto es regla de tres simple, si en vez de tener 15 servidores para proveer de aire acondicionado, UPS, etc, etc, tengo solo uno, los números se reducen bastante.

• *Mejora en la seguridad:* El poseer servidores virtuales dedicados permite tener una política de separación de servicios por servidor virtual, y en la eventualidad de que uno de estos sea comprometido, no afectará a los otros servicios, como sí sucedería si varios servicios estuvieran en el mismo servidor.

Por último es necesario aclarar que en este artículo voy a hablar fundamentalmente sobre la versión OpenSource (OSS) de Xen, es decir sobre Xen 3.1.0, y no sobre las versiones comerciales como Xen Enterprise, Xen Standard o Xen Express, salvo que haga explícita referencia a estas últimas.

FOTO: http://www.sxc.hu/ - Rodolfo Clix

¿Qué y cómo es Xen?

Xen es altamente complejo, de modo que voy a explicar su funcionamiento sin entrar en demasiados tecnicismos y tomándome ciertas licencias en favor de la claridad. Xen se compone principalmente de dos partes, el *Hypervisor* y los *Dominios*. El Hypervisor es el que "se coloca" directamente sobre el hardware, es decir que es el que administra el acceso al hardware. Xen utiliza el término Dominio para referirse a las máquinas virtuales, de todos los Dominios hay uno, el Dominio-0, que tiene lo que se podría decir que es el sistema operativo base, que es con quien se interactúa al momento de la administración. Xen soporta dos tipos de virtualización, la primera es el método de *Paravirtualización* (PV) o de sistemas operativos modificados, en este método el sistema operativo virtualizado "sabe" que está trabajando con un *Virtual Machine Monitor o VMM*. El VMM "corre" en la máquina virtual a un nivel de ejecución menos privilegiado para poder así aislar los procesos de cada una. Cuando decimos que "modificamos" el sistema operativo, lo que se modifica es el kernel que es quién se encarga de controlar los procesos y el acceso a los recursos, todo lo demás no se toca, por lo que cualquier aplicación nativa del sistema operativo no se debe modificar y funcionará como en una máquina real. El otro método de virtualización que soporta Xen es la completa o con soporte de hardware (HVM). Este tipo de virtualización permite correr sistemas operativos sin modificarlos; esta técnica es más compleja, menos veloz que la Paravirtualización y en el caso de Xen requiere que los procesadores la soporten. En este modo de virtualización no es la máquina virtual la que se corre a un nivel de ejecución menos privilegiado sino Xen se coloca en uno con más privilegios y es aquí donde el soporte por hardware entra en juego; sin este soporte esto sería imposible.

Estas dos técnicas de virtualización tienen sus puntos a favor y en contra. La PV tiene como ventajas su desempeño ya que la velocidad de ejecución que se logra con esta técnica es casi nativa y en Xen tiene soporte para más cosas como agregar y quitar recursos en caliente. Como punto en contra podemos decir que el sistema operativo tiene que ser modificado y en algunos como el caso de Windows, esto no es posible y por lo tanto nos impide correrlo como PV. La HVM tiene como gran punto a favor que no es necesario modificar el sistema operativo para correrlo y en definitiva se traduce en la cantidad de SO que podremos utilizar es mucho mayor. De hecho, casi cualquier SO que corre en la plataforma x86_32 y x86_64 corre como HVM. Como punto en contra tenemos una penalidad en desempeño derivada de la complejidad de esta técnica.

¿Qué nos permite Xen?

Xen 3.1 con sus propias herramientas nos permite:

- Correr máquinas virtuales Paravirtualizadas y virtualizadas mediante soporte de hardware (AMD Pacifica e Intel VT).
- Nos permite agregar recursos en caliente (Procesadores Virtuales, discos, memoria, interfaces de red).
- Permite el manejo de prioridades de acceso al procesador.
- Nos permite pausar y migrar máquinas virtuales en caliente y en vivo.

Utilizando otras herramientas con Xen podemos entre otras cosas:

- Migrar máquinas físicas a máquinas virtuales (tanto Linux como Windows).
- Hacer copias de respaldo en caliente de las máquinas virtuales.
- Utilizar VLANS (Standard IEEE 802.1q).
- Hacer Channel Bonding o Link Agregator (Standard IEEE 802.3ad).
- Balanceo de Carga.
- Alta Disponibilidad.
- Calidad de servicio.
- Monitoría.
- Y una larga lista de etcéteras...

Xen y Linux, una combinación imbatible

Uno de los puntos fuertes de Xen es la reutilización, principalmente la reutilización de herramientas probadas y conocidas. Entonces, ¿por qué no usarlas? Veamos algunos pocos ejemplos.

XEN CON LVM2

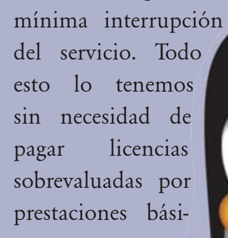
Uno de los aliados más poderosos de Xen es LVM2 y CLVM2. Para aquellos que no están familiarizados con LVM, significa Logical Volume Management y permite el manejo de volúmenes de una forma muy flexible, pudiendo crear, extender, achicar, eliminar y hacer snapshots de volúmenes en caliente. Todo esto se logra mediante la generación de una capa de abstracción entre el hardware (los discos) y el software, sin mencionar que la administración es sumamente sencilla. Por su parte CLVM2 significa Cluster Logical Volume Management y lo que nos permite es compartir los mismos volúmenes lógicos entre distintos equipos manteniendo la integridad de los datos. ¿Y qué podemos hacer con esto? Algunas cosas sumamente interesantes.

XEN CON LVM, ISCSI Y MULTIPATH

Hoy en día la calidad de las redes Ethernet permite no solo utilizarlas como una LAN tradicional sino también como un Backbone de datos, y la tecnología iSCSI combina la flexibilidad de TCP/IP con SCSI. Para quienes no están familiarizados con lo que es iSCSI en pocas palabras es el protocolo SCSI para controlar dispositivos de almacenamiento que todos conocemos, encapsulado en TCP/IP. Una solución estándar de iSCSI se compone de un Initiator o cliente y un Target o servidor. Este último se comunica con el servidor y mediante un driver hace ver localmente en el equipo los discos que están en el servidor. Para el sistema operativo no hay diferencia entre un disco SCSI interno y uno iSCSI.

Multipath no es una técnica nueva, de hecho es un tipo de RAID y funciona de forma similar al RAID 1 o mirror, con la diferencia que en un RAID multipath lo que está duplicado no es el disco sino los caminos hacia el disco -cuando digo caminos me refiero a conexiones Ethernet hasta el Target iSCSI-. Por otro lado, el disco en sí mismo es otro RAID en un Storage. También tenemos que decir que para que sea realmente efectivo el multipath, los caminos hacia ese disco tienen que ser independientes.

La combinación de Xen, iSCSI y Multipath nos da una solución robusta y de alta disponibilidad, ya que si se nos cae un disco en el storage, es un RAID y no perderemos servicio. Si se nos cae un camino al storage, utilizamos el otro y si se nos cae un servidor Xen, levantamos las máquinas virtuales en otro con una mínima interrupción del servicio. Todo esto lo tenemos sin necesidad de pagar licencias sobrevaluadas por prestaciones bási-





cas para las tecnología disponible hoy, ¿o un Target iSCSI hoy en día es una prestación de gama alta? Yo creo que no.

XEN CON FIBRE CHANNEL
Si disponemos de la infraestructura, podemos reemplazar iSCSI por Fibre Channel (FC) manteniendo los demás componentes de la solución anterior y lograremos una solución aún mejor y definitivamente High End, ya que hoy el equipamiento FC estándar permite velocidades de transferencia de 4Gb sin el overhead que puede generar el encapsulamiento en TCP/IP.

ENTORNOS FIBRE CHANNEL E ISCSI
Como otro ejemplo de la flexibilidad nativa que provee Xen con Linux es la posibilidad de mezclar también entornos FC con iSCSI, donde los equipos más críticos o con una utilización de disco mayor van a través de FC y los que hacen un uso moderado y/o bajo de disco a través de iSCSI, maximizando así la inversión en tecnología.

OTRAS OPCIONES A ISCSI Y FC
Para poder hacer migraciones en caliente de máquinas virtuales debemos sí o sí ver en ambos equipos el Storage (el o los discos) de la máquina virtual que queremos migrar. Una forma es utilizando un Storage iSCSI o FC, pero si no disponemos de por lo menos u$s 50.000 para este fin podemos también utilizar NFS, que si bien no es la solución más elegante es igualmente muy efectiva. NFS hoy en día está quedando obsoleto por la aparición de ciertos filesystems de red como el Global File System (GFS) de Red Hat que permite algo parecido pero más avanzado que NFS. GFS se utiliza sobre un dispositivo de bloques directamente, como puede ser iSCSI o un disco de un Storage FC el cual es utilizado por varios equipos concurrentemente. También como alternativa existe Oracle Cluster Filesystem (OCFS) que ofrece una funcionalidad parecida a GFS, pero debido a que con OCFS no tengo experiencia me abstengo de hablar de él.
En resumen, y como siempre con el OSS, ya que no nos "enlatamos", tenemos muchas opciones y podemos elegir y diseñar aquella solución que se adapte a nosotros y no debemos nosotros adaptarnos a las limitaciones de la "solución".

Xen 3.1 vs. VMWare

Debido a que este es un tema de consulta recurrente voy a mencionarlo, no voy a ir en detalle sobre cómo es VMWare sino voy a contar algunos puntos en los que no coinciden estos dos productos y que, desde mi punto de vista, hacen superior a Xen e hizo que en muchos ámbitos le gane la pulseada.

XEN 3.1 ES PEQUEÑO
El Kernel de Xen (el Hypervisor) ocupa aproximadamente 50.000 líneas de código o 50Kb (sí, 50kb, el 3,5 por ciento de un disquette de 3 1/2"). Si sabemos que cada 1.000 líneas de código hay un bug, vamos a tener muchos menos bugs en 50.000 líneas que si tenemos varios millones ellas.

XEN 3.1 ES FÁCILMENTE EXTENSIBLE Y ADAPTABLE
Las herramientas de Xen están hechas en Python, un lenguaje de scripting fácilmente adaptable y mantenible, lo que significa que si usted necesita algo a medida, puede contratar a una persona que sepa Python para que se lo haga y no debe sentarse a rezar que algún día su software enlatado lo incluya.

XEN NO REINVENTA LA RUEDA
Como dijimos anteriormente, Xen utiliza las herramientas de Linux probadas y súper probadas durante años para el resto de las tareas que no están directamente relacionados a la virtualización.

XEN 3.1 ES OPENSOURCE Y LIBRE
Quizás para muchas personas esto no es muy importante, pero realmente lo es. El que sea libre no es importante únicamente por una cuestión de principios, sino un hecho práctico y real que es que ninguna empresa por más grande que sea puede tener tantos desarrolladores y beta testers como la comunidad de usuarios y desarrolladores de Xen. Todo ese desarrollo y testeo fluye por la comunidad y se refleja no solo en la versión OSS sino también en las versiones comerciales. También esto se traduce en que uno puede hablar con los desarrolladores y consultarlos directamente, ¿usted cree que un desarrollador de software privativo le va a contestar un mail si no tiene la obligación? También al ser OSS no se está atado y a la merced a un proveedor monopólico que cobra lo que se le ocurre por un servicio llevado a cabo por principiantes. En definitiva todo esto se traduce en reducción de sorpresas y de costos.

Para concluir

Durante mucho tiempo la virtualización me resultó interesante, pero el software disponible no lograba satisfacer mis necesidades y expectativas ya sea por desempeño o capacidades, hasta ahora. Xen hace todo lo que se espera de un software de virtualización de forma eficiente y lo que no lo hace ya está planeado, en desarrollo o lo puede hacer uno mismo. ●

Sitios relacionados

http://xen.org
http://www.xensource.com
http://lists.xensource.com
http://www.xtech.com.ar



¿Hacia dónde va el Data Center?

Fuente: IBM

Hoy en día la información ha evolucionado de forma tal y se ha convertido en el activo más importante, con organizaciones de todo tipo confiando en los data centers como eje de sus operaciones. Veamos cuál es la tendencia y hacia dónde se dirige.

A pesar de la naturaleza del esfuerzo, el éxito depende cada vez más en el hecho de poder acceder a la información y a las aplicaciones de forma rápida y confiable y el poder obtener la información correcta de la persona correcta en el tiempo correcto.
Una rama de esta tendencia ha sido el gran aumento en la cantidad de información y aplicaciones que los data centers profesionales deben administrar. Se reportó que más de un tercio de los data centers excedían en un terabyte el tamaño de la información para finales de 2006, y nueve de diez esperaban que sus operaciones crecieran durante el año siguiente. Y como los presupuestos dentro de IT aumentaron en 2007 más de lo esperado, a los administradores de los data centers se les pide más por menos.

A continuación les mostramos algunas de las cuestiones que actualmente afectan a los data centers.

1. Gran aumento del volumen de la información. Se proyecta que la base de información del mundo -el material crudo para las bases de datos- se duplicará cada 11 horas en 2010, con la obvia implicancia en los data centers. Ya hoy en día la cantidad de información transmitida globalmente a través de Internet es duplicada anualmente y continuará de esta forma hasta por lo menos los próximos cinco años, según afirmó la empresa de investigaciones IDC.
Muchos factores contribuyen a este crecimiento, incluyendo el aumento de las transacciones con clientes, proliferación de nuevos dispositivos, problemas de conformidad, aumento de la performance de los sistemas, iniciativas de negocios en línea y el aumento de la duplicación en sitios secundarios o de back up.

2. Un renovado interés en mainframes. Los mainframes modernos pueden bajar los costos y la complejidad de los data centers. Tienen el potencial de beneficiar la confianza y la disponibilidad así como también brindar mayores niveles de escalabilidad y administración. Comparado con clusters de servidores pequeños, los mainframes actuales representan un ahorro en el costo, reducción de las interrupciones, mayor facilidad de uso y una disminución en la complejidad.
Un artículo de Sine Nomine Associates afirma que "los mainframes, como el System z de IBM, se consolida con la virtualización hasta su límite lógico, concentrando decenas, cientos y hasta miles de servidores en una sola máquina física". A pesar de las predicciones de los analistas de Gartner para 2007, la venta de mainframes es un éxito gracias al proceso de conformación, un nuevo sistema abierto de cantidad de trabajo, hardware más barato, menor necesidad de potencia y de enfriamiento.

3. Más popularidad de los servidores blade y el desarrollo de uno nuevo con una infraestructura específica de energía y enfriamiento. La última generación de servidores blade combinan un aumento en la densidad de pro

cesamiento junto con un ahorro de energía de entre el 20 y el 30 por ciento respecto a modelos anteriores, mientras además brindan flexibilidad y versatilidad a la demanda de los data centers. Garner Dataquest proyecta que el transporte de servidores aumentará hasta 2.3 millones de unidades para 2011, alcanzando el 22 por ciento de las compras de servidores hasta ese momento. Sin embargo, aún con el ahorro de energía de los nuevos modelos, los servidores blade demandan de mucho hardware en lo que se refiere a energía y enfriamiento. Por tanto los proveedores comenzaron a introducir energía modular y adaptable y sistemas de enfriamiento diseñados específicamente para satisfacer las necesidades de los servidores blade.

4. El desarrollo de aplicaciones de servidores se traslada de la periferia del negocio al centro de las operaciones del data center. Aunque se use o no la terminología, las redes que se mueven en esta dirección están adoptando los principios de SOA (Service Oriented Architecture). Las aplicaciones de arquitectura centrada en el servidor están siendo adoptadas rápidamente en data centers. Las soluciones basadas en esa arquitectura están ubicadas en algún lugar del core en hasta el 80 por ciento de los data centers. Históricamente, el énfasis en SOA ha sido mucho más en la tecnología en vez de en la solución, pero la tendencia actual refleja que el foco se está moviendo de la aplicación a la administración, monitoreo y mejora de las aplicaciones.

5. El costo es la principal preocupación de la administración de los data centers. Más de la mitad de los managers de data centers consideran como una de sus mayores preocupaciones el reducir los costos operacionales. Sin embargo, consideran mejorar el negocio, escalar la capacidad de soportar el crecimiento del negocio y aumentar los niveles de servicios. Como resultado, muchos de ellos se encuentran luchando con el querer mejorar la performance del data center junto con las dificultades financieras que esto acarrea. Además de los desafíos relacionados con los costos, deberán hacer malabares con el espacio, la energía, el enfriamiento, la administración y amortización del equipo y el personal.

6. Aumento de la demanda de métricas para medir la performance del data center. Las buenas decisiones de administración están sujetas a la habilidad de medir con precisión la performance, y los managers de los data centers están ganando acceso para tener mayores recursos en esta área. Entre ellos el sistema de cuatro niveles del Uptime Institute que mide la confiabilidad en situaciones críticas del data center y el sistema de clasificación Criticality Levels del Syska Hennessy Group, el cual incorpora la disponibilidad esperable y la confiabilidad entre los sitios que fueron diseñados, construidos, mantenidos y operados en diferentes niveles de prioridad.
Un grupo de profesionales, incluyendo la American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), comenzó a publicar estándares universales para ayudar en el planeamiento del espacio de los data centers. Publicaciones como Liquid Cooling Guidelines for Datacom Equipment Centers de ASHRAE son el primer paso para lograr un estándar acabado en el diseño de data centers.
Adicionalmente, EPA está trabajando en un extenso conjunto de benchmarks para servidores y data centers, estimando el ahorro de costos de los equipos de IT y del impacto potencial de la eficiencia de la energía en la performance del producto y a través de la cadena de suministros.

7. Los cambio en los entornos virtuales están llevando a la necesidad de la configuración de la administración de las bases de datos, y la administración general del entorno virtualizado necesita ser mejorado a través de un sistema de administración de niveles más bajos. La automatización de la configuración de la administración de la base de datos no significaba un gran problema en los tiempos del mainframe. Las plataformas propietarias tenían un robusto proceso de administración y era más fácil administrarla manualmente. Las aplicaciones de servidores dispuestas en racks tienen una caja dedicada que se puede cambiar en caso de que surja algún problema. Sin embargo, en un entorno virtualizado múltiples aplicaciones corren en una infraestructura compartida, lo que representa pequeños problemas-muchos de los cuales son causados por el cambio. La configuración de la administración de las bases de datos ayuda a los usuarios a alinear la administración de su infraestructura de IT con las prioridades de su negocio en un entorno virtual.
En el nivel de la administración del sistema, IBM ofrece algunas de las mejores herramientas de hardware existente en la industria, diseñada para ahorrar tiempo y dinero mientras aumenta la disponibilidad, optimizando la performance y permitiendo el mantenimiento remoto. IBM Director, una solución de administración líder en la industria, es una suite abierta e integrada de herramientas de software que brindan consistencia, un solo punto de administración y automatización.

“El COSTO es la PRINCIPAL PREOCUPACIÓN de la administración DE LOS DATA CENTERS”

8. Aumentar el foco en los problemas de energía, incluyendo la articulación entre hardware y empresas de servicios públicos para las actualizaciones de los equipos. El costo es uno de los factores más importantes, pero la principal preocupación es la restricción a las operaciones y al aumento del consumo de energía de los equipos de IT. El costo de la energía es el segundo ítem asociado con las operaciones del data center y se espera que aumente en un 50 por ciento el presupuesto total en los próximos años. Gartner proyecta que la mitad de los managers de IT no tendrán la energía suficiente como para correr sus data centers en 2008.
Las empresas de servicios públicos y los vendors de software y hardware se están asociando para ayudar a los usuarios finales a reducir el consumo de energía, generalmente bajo programas como el Climate Saver Computing Initiative. El CSCI trabaja junto con la industria, los consumidores, el gobierno y las or-

ganizaciones para aumentar la eficiencia de la energía de las computadoras y los servidores.

9. Aumentar el foco en los problemas de seguridad tanto para las aplicaciones como para la información. Los administradores de los data centers enfrentan grandes desafíos en este frente, desde la protección de la información y las aplicaciones de los accesos no autorizados pasando por la seguridad de las interacciones en la red hasta la seguridad física de la infraestructura y un plan para la recuperación en caso de desastre. Entre los problemas que más preocupan a los administradores y managers de IT de medianas empresas, según una encuesta realizada por IDC en 2006, la seguridad es la principal.

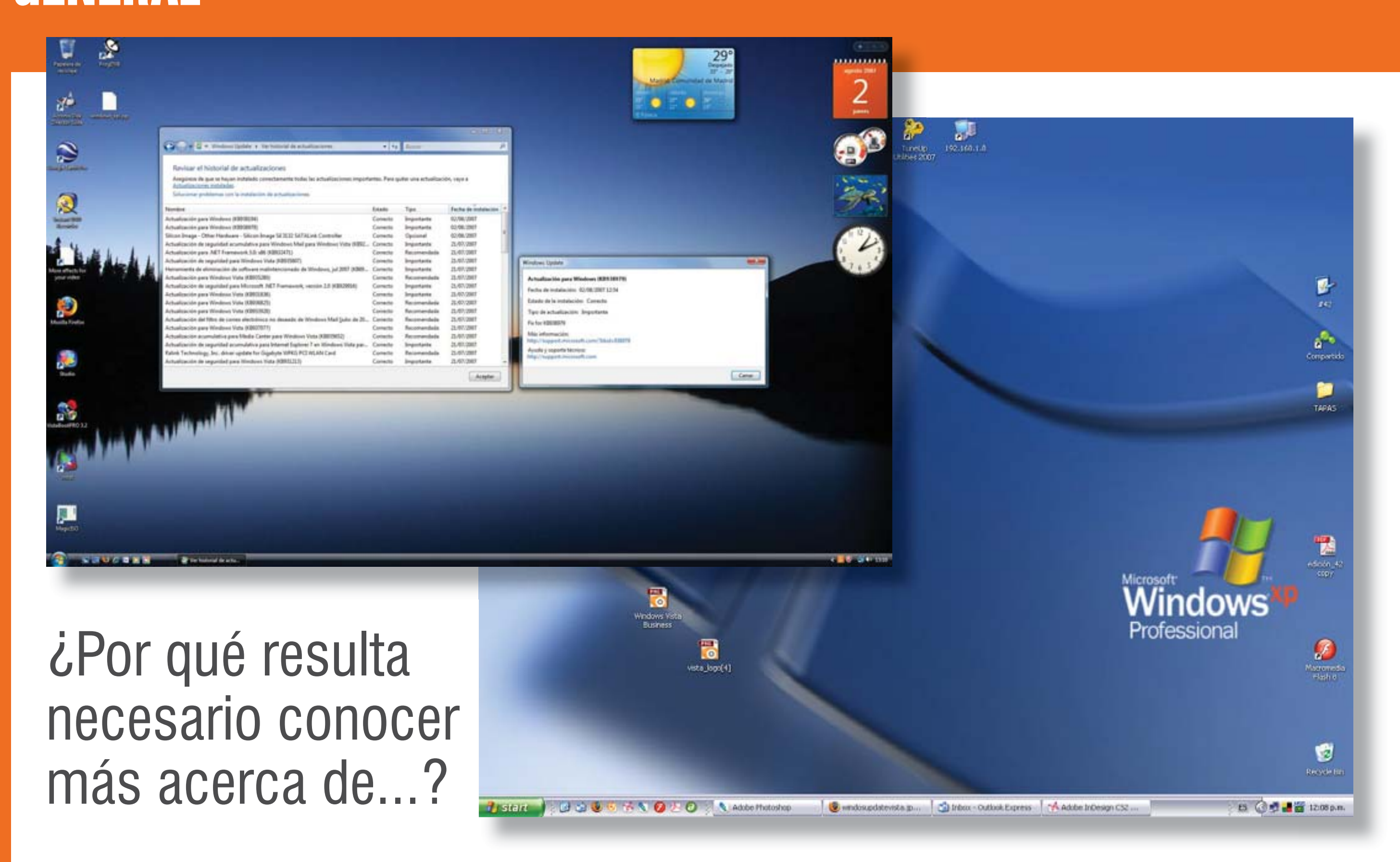
Mientras existe un determinado grado de subjetividad en listas como estas, también hay dudas acerca de si estas tendencias tendrán un papel principal en la evolución de los data centers. Como el filósofo griego Heráclito dijo hace 2.500 años atrás “Todo fluye, nada se queda quieto”. ●







FOTO: http:// www.sxc.hu - Justin Fitzpatrick - Philippe Ramakers



¿Por qué resulta necesario conocer más acerca de...?

WINDOWS
Preinstallation Environment

Cuánto tiempo tarda Usted en efectuar una instalación si es profesional de sistemas. Y cuántas veces repite dicho proceso en la reinstalación.

Daniel M. Salazar

Piense por un momento (aunque nos cueste creerlo) que puede realizar este proceso una sola vez y a partir de allí generar una imagen de la instalación, incluyendo drivers y programas utilitarios como por ejemplo Microsoft Office. A partir de dicha imagen Ud. puede efectuar una instalación desatendida en múltiples equipos en solo 10 minutos y dejar el sistema completamente utilizable.

Con la ventaja para los integradores OEM de poder personalizar las pantallas de bienvenida a los equipos con sus logos y ofertas para los clientes.

Descripción de la implementación de Windows Vista

El término implementación se refiere a la instalación del sistema operativo Windows Vista en equipos cliente a través de una red. La diferencia entre implementación e instalación básicamente es de escala. El segundo término describe la instalación del sistema operativo en un único equipo, casi siempre mediante la interacción directa con el software y el hardware del mismo. Las implementaciones generalmente se realizan en varios equipos al mismo tiempo, con frecuencia mediante secuencias de comandos de configuración personalizadas. Windows Vista presenta algunas

Característica	Descripción
XImage.exe	Herramienta de la línea de comandos para crear y aplicar archivos de imágenes de Windows.
Windows Imaging (WIM)	Nuevo formato de archivo para imágenes.
Windows Deployment Services (WDS)	Servicios de implementación de Windows que reemplazan a los servicios de instalación remota (RIS) en la implementación de Windows.
Windows Preinstallation Environment (Windows PE)	Entorno de preinstalación de Windows con métodos de inicio adicionales compatibles para las instalaciones cliente OEM o Enterprise.
Windows Setup Manager	La administración de instalación de Windows es una herramienta gráfica y de línea de comandos para el mantenimiento de los archivos de imágenes de Windows.
Unattend.xml	Nuevo formato de secuencia de comandos para todas las instalaciones basadas en imágenes de Windows Vista.
System Preparation (SysPrep)	Herramienta de preparación del sistema con un funcionamiento mejorado para operar con el diseño modular y la instalación basada en imágenes.

nuevas tecnologías que simplifican el proceso de implementación en varios equipos cliente.

Novedades en la implementación

La instalación basada en imágenes (Image-based Setup, IBS) es el nuevo mecanismo de implementación de sistemas operativos para la instalación de Windows Vista. Proporciona una arquitectura de instalación común que simplifica y acelera el proceso para los usuarios, al tiempo que permite aplicar los métodos de implementación más comúnmente utilizados por las organizaciones y los fabricantes de equipos. Entre las nuevas características de la instalación de Windows Vista se incluyen las siguientes:

Ventajas de la implementación

La sola instalación basada en imágenes (IBS) constituye una ventaja significativa sobre los métodos de implementación de Windows anteriores. Con las nuevas tecnologías de implementación de imágenes de disco se puede crear, mantener e implementar Windows Vista sin necesidad de software de imágenes de disco adicional.

Preparación de la imagen

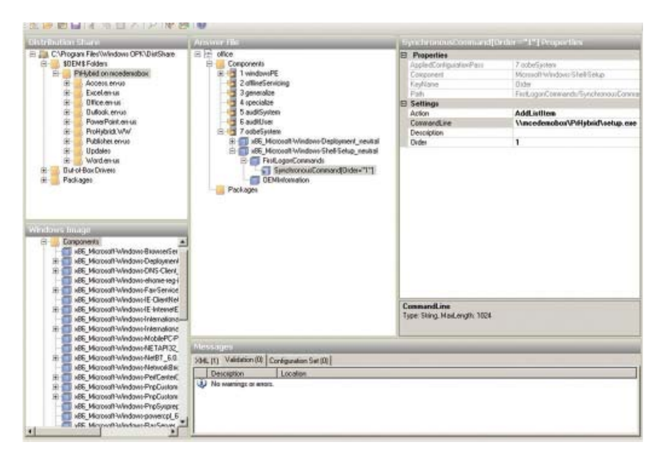
Una imagen de implementación contiene idealmente el sistema operativo y la configuración estándar de las aplicaciones del entorno de red. El primer paso es crear la configuración que se va a implementar. Utilice el equipo principal designado para crear la configuración. Instale la versión de Windows Vista en el equipo y cualquier aplicación que desee implementar como parte de la imagen. Configure el sistema operativo y las aplicaciones de acuerdo con los estándares deseados y ejecute SysPrep para eliminar cualquier Id de seguridad (SID) único del equipo principal.

Captura de una instalación completa

Si captura una instalación completa, la mejor alternativa es iniciar el equipo desde Windows PE. Dado que Windows PE se ejecuta en memoria o desde un CD o DVD, se garantiza que no se incluye en la imagen de instalación nin-

El **Microsoft Windows Preinstallation Environment** (Windows PE) le brinda más **herramientas de instalación y preparación** para Microsoft Windows XP Professional y Microsoft Windows Server 2003 de forma de **facilitarle la tarea a los profesionales del área de IT**.





gún archivo o carpeta bloqueados. Los archivos y carpetas bloqueados podrían ocasionar errores en la captura de la imagen.

Uso de SysPrep

La herramienta de preparación del sistema elimina de un equipo la información de identificación única antes de capturar la imagen de dicha instalación para su implementación. La ventaja de esta herramienta es que permite instalar y configurar Windows Vista y distintas aplicaciones y a continuación eliminar los identificadores únicos para que la imagen resultante se pueda instalar en varios equipos sin crear conflictos de identificación.

SysPrep pasa por 6 fases distintas:

• **Comprobación:** Antes de que realice cualquier cambio en la configuración de la instalación principal, SysPrep comprueba distintas opciones y recopila información sobre la misma.

• **Inicialización:** La inicialización implica comprobar que el protector de pantalla no está habilitado. Si lo está, SysPrep lo deshabilita y guarda la configuración para que se pueda volver a activar y configurar durante el inicio de Windows.

• **Configuración:** El proceso de configuración implica lo siguiente:

- Comprobar la sintaxis de los comandos.
- Mostrar un cuadro de diálogo en el que se describe la herramienta SysPrep. Los usuarios deben asegurarse de que se lee este mensaje. Este proceso se omite si se utiliza el nivel no interactivo.

• **Ejecución principal:** El proceso de ejecución principal incluye lo siguiente:

- Ejecutar las opciones seleccionadas. La ejecución principal se divide en tres fases: generalización, especialización y limpieza. Durante la ejecución principal se cargan los componentes y los controladores necesarios.
- Registrar cualquier error en un archivo de registro local (%SYSTEMROOT%\SysPrep\Panther\Setupact.log).

• **Terminación:** El proceso de terminación implica lo siguiente:

- Ejecutar las opciones de terminación seleccionadas (/quit, /reboot y /shutdown).
- Establecer el indicador que señala que la operación se ha realizado correctamente.

• **Finalización:** El proceso de finalización implica lo siguiente:

- Eliminar los registros de sucesos.
- Eliminar la configuración específica de cada usuario, como las opciones del Reproductor de Windows Media y el asistente para la conexión a Internet.
- Eliminar la lista de documentos, aplicaciones y sitios Web más recientes.

Para ejecutar SysPrep en el equipo principal:

1. En el símbolo del sistema, abra la carpeta SysPrep. Por ejemplo, escriba:

Cd C:\opk\tools\SysPrep

2. Para ejecutar SysPrep y preparar el equipo para la captura de la imagen, escriba lo siguiente: **Sysprep.exe /image**

Si el equipo principal no se cerrara correctamente después de ejecutarse SysPrep, agregue el modificador /shutdown a la línea de comandos. Consulte el kit de instalación automatizada de Windows (WAIK) o el kit de preinstalación de OEM (OPK) para obtener la sintaxis de comandos completa de SysPrep.

Captura de la imagen

XImage permite capturar la imagen con una compresión rápida. Una vez capturada, la imagen se puede modificar y aplicar a la red o a los equipos de destino.

Para capturar una imagen con la compresión máxima:

1. Inicie el equipo principal con Windows PE.
2. En el símbolo del sistema, abra el directorio XImage. Por ejemplo, escriba: c:\opktools\ximage
3. Para capturar la imagen, escriba: ximage /capture d:\image_directory c:\imaging\data.wim “Nuevo_archivo_imagen”

d:\Image_Directory es la ubicación de los archivos de los que se va a crear una imagen, c:\Imaging\Data.wim es el nombre y la ubicación del nuevo archivo de imagen y “Nuevo_archivo_imagen” es una descripción del archivo de imagen.

Mantenimiento de la imagen

Una vez que se cuenta con el archivo de imágenes de Windows (.wim), se puede asignar el contenido de la imagen a un directorio (montar) y realizar operaciones de archivo comunes, como copiar, pegar y editar mediante una herramienta de administración de archivos como el explorador de Windows sin necesidad de extraer o volver a crear la imagen.

Windows PE es un **mínimo sistema de Windows** que **brinda servicios limitados** basado en el kernel de Windows XP Professional y Windows Server 2003. Además ofrece el conjunto de **características mínimas requeridas** para correr Windows Setup, la instalación y el **acceso al sistema operativo desde la red** y el **hardware validado**.

Para manipular una imagen es preciso instalar el controlador del filtro del sistema de archivos de imágenes de Windows (WIM FS Filter) en el equipo técnico. Cuando se ha instalado, el controlador permite montar la imagen con permisos de sólo lectura o de lectura y escritura y ver los archivos y carpetas que incluye con una herramienta de administración de archivos como el explorador de Windows.
Para poder montar o modificar la imagen es preciso instalar el controlador de WIM FS Filter en el equipo técnico.

Instalación del controlador del filtro

1. En el explorador de Windows, abra el directorio XImage. Por ejemplo, vaya a: **c:\opk\tools\ximage**
2. Haga clic con el botón secundario del mouse en el archivo **Wimfltr.inf** y, a continuación, elija Install (Instalar).

Montaje de una imagen

Después de instalar el controlador de WIM FS Filter puede montar la imagen con permisos de sólo lectura o de lectura y escritura en un directorio en el equipo técnico. Si la monta con permiso de sólo lectura, no podrá modificar la imagen ni guardar cambios.

¡Atención!

Después de montar la imagen, los archivos o carpetas existentes en el directorio de montaje desaparecen. Volverán a aparecer cuando desmonte el directorio.
Para montar una imagen con permisos de lectura y escritura
1. Inicie el equipo técnico con un sistema operativo Windows compatible.
2. En el símbolo del sistema, abra el directorio XImage. Por ejemplo, escriba:
Cd c:\opk\tools\ximage
3. Para montar la imagen, escriba: ximage /mountrw c:\mounted_images d:\imaging\data.wim 2
4. c:\Mounted_Images es la ubicación del directorio de montaje, d:\Imaging\Data.wim es el nombre y la ubicación del archivo .wim que se va a montar y 2 es el número de referencia del volumen específico en el archivo .wim.

Modificación de una imagen

Una vez que se ha montado la imagen, la estructura del directorio se encuentra disponible desde una herramienta de administración de archivos, como el explorador de Windows. Con dicha herramienta se puede revisar la estructura de archivos y carpetas, agregar archivos y carpetas, modificar los existentes y eliminar cualquiera que no se necesite.

Para ver archivos y carpetas

1. Desde el equipo técnico, inicie el explorador de Windows y abra el directorio montado. Por ejemplo, vaya a: c:\mounted_images
2. Revise la estructura de archivos y carpetas, incluido su contenido.

Nota

Si debe agregar una aplicación o dispositivo, compruebe que ha incluido todos los archivos necesarios. Aunque se permite agregar carpetas y archivos de aplicación, no se pueden instalar aplicaciones.

Desmontaje de una imagen

Tras modificar una imagen, ésta se debe desmontar. En este momento, si la imagen se ha montado con permisos de lectura y escritura, los cambios se pueden aplicar sin problemas y las modificaciones se pueden convertir en parte permanente de la misma.

Nota

No ejecute la opción /unmount /commit desde Windows PE. Dado que Windows PE obliga a que el equipo se reinicie cada 24 horas y puesto que las imágenes montadas no se pueden guardar entre reinicios, si debe aplicar cambios en el sistema de archivos cuando el equipo se reinicie, dichos cambios se perderán.

Para desmontar una imagen

1. Inicie el equipo técnico con un sistema operativo Windows compatible.
2. En el símbolo del sistema, abra el directorio XImage. Por ejemplo, escriba:
c:\opktools\ximage
3. Para desmontar la imagen, escriba:
ximage /unmount /commit c:\mounted_images
c:\Mounted_Images es la ubicación del directorio de montaje. Si no especifica los parámetros que desea desmontar, esta opción enumera todas las imágenes montadas, pero no realiza la operación de desmontaje.

Aplicación manual de la imagen

Puede utilizar XImage para aplicar manualmente una imagen de implementación como imagen de prueba a un equipo. Para hacerlo desde un archivo WIM, es preciso preparar primero el equipo de destino creando y formateando las particiones de disco, a menos que la intención sea ejecutar los comandos desde una secuencia. Si elige realizar estas tareas desde una secuencia de comandos, inserte los comandos para crear y formatear las particiones de disco antes de los comandos de Ximage para aplicar la imagen.
La sintaxis de los comandos para aplicar una imagen mediante XImage es la siguiente:
Ximage [/apply image_file directory index_number [/verify]].

Acerca del Autor

DANIEL M. SALAZAR
MCP – MCTS SQL 2005
Oxford´s University FCIC
Microsoft Senior Trainer
Microsoft New Tech Evangelist

Webcast y lectura adicional

http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032293463&CountryCode=US

http://technet.microsoft.com/en-us/windowsvista/aa905061.aspx



Protección contra las vulnerabilidades

*Este artículo ha sido publicado en el Newsletter de Seguridad Microsoft de Octubre 2007.

Cuando de Protección contra las Vulnerabilidades se Trata, el Proceso No Respeta a una "Mayor Cantidad de Observadores".

Pat Edmonds
Gerente de Producción Senior
Microsoft Corporation

Existen diferencias en la forma en que los modelos del Servidor de Windows y el de Linux son desarrollados. Microsoft pone el énfasis en la implementación de un modelo de desarrollo que permita la inclusión de los atributos del software de importancia en el proceso de planificación. Un ejemplo muy claro de esto es la interoperabilidad.

Estas diferencias en modelos también se pueden traducir a las diferencias de seguridad en el mundo real para los clientes:

• Cómo se identifican, informan y reparan los errores/virus.
• La reducción de la severidad de las vulnerabilidades.
• La reducción del total de Días de Riesgo para Windows en relación a Linux.

La seguridad es a menudo considerada como de suma importancia al momento de la decisión de compra del sistema operativo de un servidor. La realidad es que los Servidores de Linux y de Windows tienen filosofías muy diferentes sobre la seguridad de la información, que se traducen en experiencias diferentes para sus clientes. Luego de años de construir y mejorar un enfoque céntrico del proceso para el desarrollo de la seguridad, resulta claro que el modelo del Ciclo de Vida del Desarrollo de la Seguridad de Microsoft contribuye a que la plataforma del servidor de Windows sea altamente segura para cualquier empresa.

Nadie precisa decirle a los CIOs que los riesgos a la seguridad de la información son cada vez más altos. De acuerdo con Forrester, un 10 por ciento promedio de los presupuestos de TI son destinados a la seguridad, y por una buena razón. Por ejemplo:

• Un estudio reciente de Consumer Reports estima que los esquemas de los virus de Internet, spyware y phishing (fraude electrónico) le han costado a los consumidores de los EE.UU. más de 7 billones de dólares en los últimos dos años, y que la oportunidad de convertirse en una víctima cibernética es de 1 en 4.

• Un estudio de la Enterprise Management Asociates de seis compañías con datos revelados por violaciones a la seguridad hace notar que el precio promedio de estas compañías disminuyó en un 5 por ciento al décimo sexto día hábil luego de la revelación. Para las cuatro compañías cuyos precios en las acciones pueden ser rastreados hasta hace un año atrás, sus promedios permanecieron dentro de un rango del -2,4 al 8,5 por ciento hasta 195 días hábiles subsiguientes al episodio. En la figura 1 las líneas en colores representan las compañías analizadas objeto del estudio.

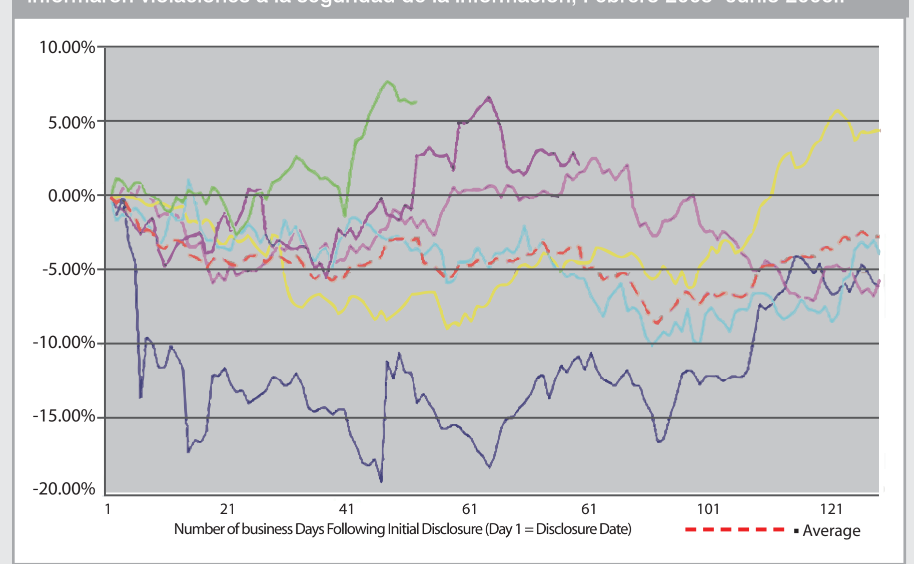
Cuando nos referimos a contrarrestar las amenazas a la seguridad, Windows y Linux adoptan enfoques diferentes. Tanto los vendedores de Microsoft como aquellos de la compañía líder Linux podrían utilizar un número de técnicas y herramientas de seguridad probadas similares, pero las filosofías de desarrollo de Windows y Linux son divergentes.

Por ejemplo, las distribuciones de Linux siguen el modelo de desarrollo de código abierto. Dependiendo de las intenciones y las habilidades del usuario, Linux puede personalizarse tornándose extremadamente seguro. Con esta capacidad de personalización, sin embargo, se conlleva la responsabilidad en aumento por parte del usuario de asegurar el código. Las distribuciones más importantes soportadas por Linux tienen provisiones en sus contratos para parar su soporte del producto, incluyendo el soporte de seguridad como administración de parches, una vez que el código ha sido personalizado más allá de cierto punto.

Además, existe una percepción generalizada dentro de la comunidad Linux: "los ojos de muchos observadores hacen que los virus pier-

FOTO: http://www.sxc.hu/ - Ruud van de Schoot

Fig. 1 - Cambios en los precios de cierre de las acciones de las seis compañías que informaron violaciones a la seguridad de la información, Febrero 2005- Junio 2006..



dan su fuerza", una referencia a la creencia de que la naturaleza comunitaria de Linux y su código abierto y visible alientan y permiten a que un mayor número de usuarios identifiquen virus y errores y ofrezcan las recomendaciones para la resolución de los problemas que estos presentan. En realidad, el mantra de la "mayor cantidad de observadores" para la seguridad de Linux ha sido ampliamente desaprobado por dos razones primordiales. Primero, asume que todos los "ojos observadores" se encuentran calificados para saber que están buscando. En realidad, la pericia en el área de seguridad no es mayormente conocida entre la mayoría de los usuarios y constituye un grupo de habilidades y prácticas bastante raras y valoradas. Segundo, el argumento del "mayor número de observadores" implica que todos los "ojos de los observadores" quieran en forma voluntaria examinar con detenimiento el código en busca de virus y errores. En realidad, la resolución de problemas y el código de evaluación no son necesariamente uno de los pasatiempos más excitantes para muchos desarrolladores voluntarios, quienes preferirán dedicar su tiempo libre a la creación de la próxima gran aplicación. Como resultado, no es sorprendente que Ben Laurie, Director de Seguridad de la Fundación Apache, haya dicho que "aunque todavía es usado a menudo como un argumento, me parece bastante claro que el argumento de la 'mayor cantidad de ojos observadores', no se aplica al tema de la seguridad".

La falta de un enfoque céntrico de proceso sobre la administración de seguridad parece estar al día con el desarrollo de Linux, dado que Linux se convierte en un proceso más complejo día a día. Andrew Morton, Líder Mantenedor del Kernel de Linux, ha dejado entrever:

Dadas las diferencias obvias en el enfoque de la seguridad que Linux y Windows poseen,

"Creo que el kernel 2.6 se está llenando de virus lentamente. Parece que estamos agregando virus a una tasa mayor de la que los estamos reparando". También notó que algunos pocos desarrolladores se encuentran motivados a trabajar para reparar virus y errores. Jonathan Corbet, co-fundador de LWN.net, comentó recientemente que "los desarrolladores de Linux parecen permitir que los informes de los virus y errores se deslicen a través de las fracturas. Con 1.500 virus de núcleo en el sistema de rastreo, y 50 sin respuesta en la lista de correo, ¿precisan los desarrolladores un mejor proceso o tan sólo nuevas prioridades?".

A diferencia del modelo de Linux, Microsoft promociona la seguridad de sus productos a través del Ciclo de Vida de Desarrollo de Seguridad (Security Development Lifecycle o SDL). El SDL surgió de un famoso memorando de Bill Gates de 1992 que marcaba el curso de Microsoft en dirección a convertirse en un líder en el área de la seguridad después de años de (generalmente justificadas) preocupaciones de clientes sobre el compromiso de Microsoft para con la seguridad. El propósito del SDL es doble: reducir el número de vulnerabilidades en el código y reducir la severidad de los virus que se filtran por él. Dado que es virtualmente imposible atrapar todas las vulnerabilidades, la clave consiste en asegurar un proceso disciplinado capaz de identificación y corrección de los virus y errores de la forma más adecuada y priorizada que sea posible.

La ventaja del SDL consiste en que la seguridad es "cocinada dentro" de los productos de Microsoft a cada paso del desarrollo a través de una serie de portales y controles severos de seguridad realizados por expertos. La seguridad también se ve reforzada en el desarrollo del producto a través de las amplias inversiones que Microsoft continúa realizando en el área de capacitación para la seguridad y la priorización ejecutiva de arriba a abajo para asegurarse que esta sea parte de la cultura corporativa. Como parte de este compromiso, Microsoft invirtió más de 200 millones de dólares en la capacitación de más de 13 mil empleados de Windows en técnicas de desarrollo centradas en la seguridad y nuevos procesos de ingeniería, resultando en una revisión de la seguridad línea por línea del Servidor de Windows 2003. En un giro del modelo de Linux de "muchos ojos observadores", Microsoft a menudo realiza versiones de pre-lanzamiento de su software disponible y tiene un amplio programa interno de "autoalimentación de seguimiento" para que los empleados evalúen los betas y brinden información al respecto. Por ejemplo, más de 2.25 millones de copias de prelanzamiento del Windows Vista fueron distribuidas para ayudar a asegurar su estabilidad y que cumpliese con los requisitos del mundo real.

Diferente al modelo de "muchos ojos observadores" de Linux, los productos de Microsoft son probados por un número de profesionales dedicados cuyo sustento se basa en su capacidad para encontrar y solucionar problemas en los códigos. Dicho de otro modo, más de 2.500 evaluadores llevan a cabo evaluaciones y pruebas del Servidor de Windows 2003 (Windows Server 2003).

La seguridad no termina con el desarrollo del SDL. Cuando surge un problema con un software, los clientes pueden enviar un informe anónimo a Microsoft. Los temas relacionados con la falla en los sistemas involucran el servicio de Análisis de Caídas en Línea de Microsoft, que realiza una investigación e informa más en detalle. Los datos son utilizados para mejorar los últimos productos, y de ese modo reforzar las lecciones aprendidas en lanzamientos futuros y manejar un ciclo de seguridad de mejora continua.

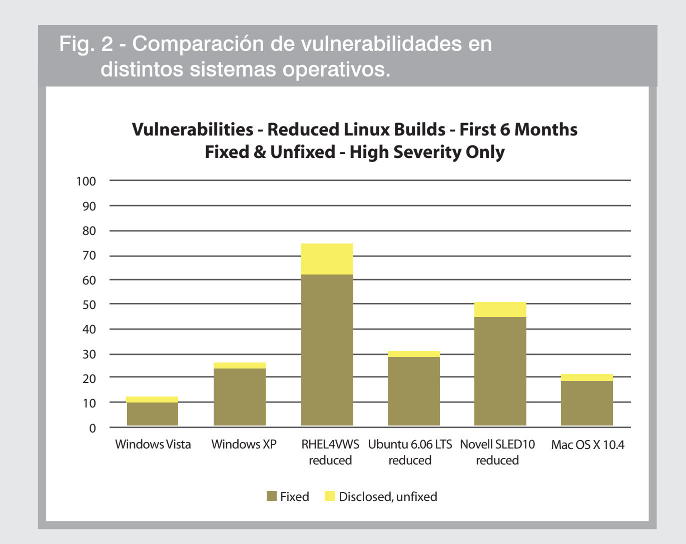
Un área de seguridad en la que Microsoft se ha dejado estar detrás de Linux ha sido la habilidad de esta última para personalizar las distribuciones para excluir componentes innecesarios, y por este medio reducir el área de superficie de la vulnerabilidad del producto. Con el Servidor de Windows 2008, Microsoft ha dado un gran paso en la misma dirección permitiendo a los usuarios desmontar aplicaciones innecesarias para reducir el área de superficie de vulnerabilidad a través del Núcleo del Servidor.

La instalación del Núcleo del Servidor es tan sólo una fracción del tamaño de la Instalación del Servidor de Windows porque excluye un número de características de Windows tradicionales, incluyendo la interfaz del usuario gráfico de Windows (a excepción de una capacidad de un conjunto mínimo de gráficos), el Microsoft Internet Explorer y el Windows File Explorer.

Dadas las diferencias obvias en el enfoque de la seguridad que Linux y Windows poseen, ¿qué resultados brindan éstos a los clientes? Mediante cualquier tipo de medida, el SDL ha brindado a los clientes de Windows menor cantidad de vulnerabilidades en los sistemas operativos. En una comparación recientemente llevada a cabo de las vulnerabilidades en los sistemas operativos en cuestión durante los primeros seis meses de sus lanzamientos, el Windows Vista tuvo bastante menos vulnerabilidades que sus rivales de Linux. Además, a modo de evidencia adicional del ciclo de mejora continua generado por el SDL, el Windows Vista también tuvo menos de la mitad del número de vulnerabilidades que su predecesor, el Windows XP, tuvo a los seis meses de su lanzamiento (ver figura 2).

De la misma manera, una comparación de las vulnerabilidades entre el Windows Server 2003

Fig. 2 - Comparación de vulnerabilidades en distintos sistemas operativos.



¿qué resultados brindan éstos a los clientes?



y sus rivales empresariales de Linux desde enero a julio de 2007 mostraron que el Windows Server 2003 tuvo muchas menos vulnerabilidades, incluyendo menor cantidad de vulnerabilidades de alta criticidad (ver figura 3).

Al comparar la seguridad entre diferentes productos, una medida común de la vulnerabilidad es la de los Días de Riesgo (DoR). Las DoR miden el tiempo desde el cual la vulnerabilidad ha sido públicamente dada a conocer hasta que una actualización de un proveedor se encuentra disponible para dar fin a dicha vulnerabilidad. En una comparación de Microsoft, Red Hat, Novell, Sun y Apple llevada a cabo en el 2006 con respecto al promedio de Días de Riesgo, Windows demostró nuevamente ser más seguro que sus rivales, incluyendo sus rivales de Linux. El análisis agregó múltiples versiones de productos para cada proveedor dado que muchos clientes habían implementado varias versiones. Los resultados indican que, en promedio general los clientes que utilizan el Windows arriesgan exponerse a las vulnerabilidades, incluyendo aquellas del tipo de gran criticidad, por un período significativamente más corto de tiempo que aquellos quienes utilizan los sistemas operativos del rival. El Novell Enterprise Linux tuvo un DoR promedio de más de 2.5 de duración que el de Windows, y el Red Hat Enterprise Linux tuvo un DoR promedio de casi 4 veces más de duración que el de Windows. Además, los clientes del Novell Enterprise Linux fueron expuestos a vulnerabilidades del tipo severo casi dos veces más frecuentemente que los usuarios de Windows, y los clientes del Red Hat Enterprise Linux fueron expuestos a vulnerabilidades del tipo de alta criticidad con una frecuencia en más de 3 veces que los usuarios de Windows.

Windows y Linux son desarrollados y soportados a través de diferentes modelos, y estos enfoques divergentes llevan a diferentes experiencias de seguridad e interoperabilidad para los usuarios finales. En la elección entre el Windows y el Linux, el enfoque céntrico del proceso SDL disciplinado así como la interoperabilidad por diseño, han permitido que el modelo de desarrollo de Microsoft ofrezca beneficios convincentes para los clientes. El enfoque de Microsoft brinda a los clientes elecciones reales en lo que se refiere a estructura y les brinda seguridad en cuanto a las elecciones que estos realicen. ●

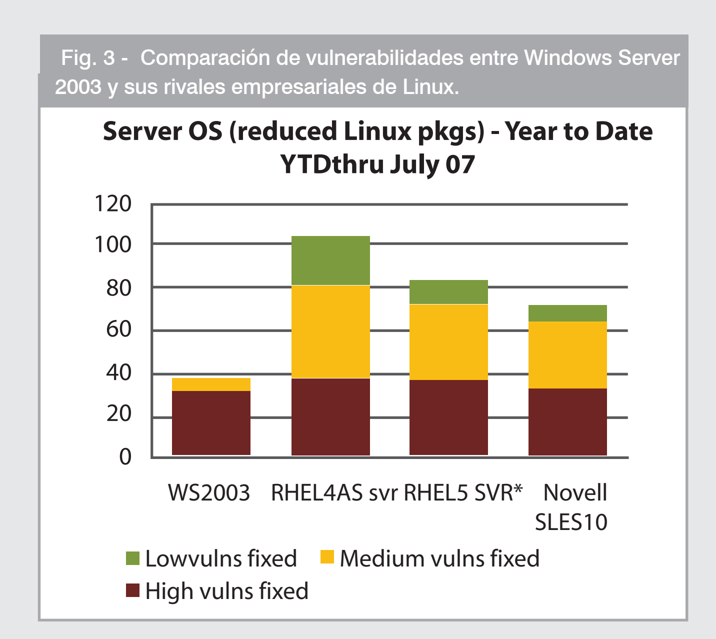


Fig. 3 - Comparación de vulnerabilidades entre Windows Server 2003 y sus rivales empresariales de Linux.

Más información

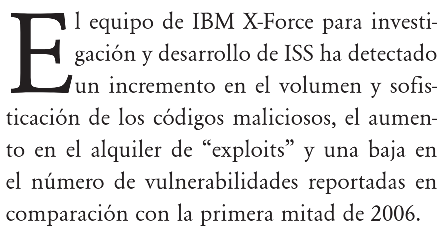
Sobre la comparación de la seguridad ofrecida por Microsoft y Linux visite http://www.microsoft.com/windowsserver/compare/linux/security.mspx

Cyber Attacks en crecimiento

2007 ha sido un año muy interesante e inusual en muchos frentes de la seguridad informática. El grupo de investigación y desarrollo de IBM Internet Security Systems X-Force ha descubierto, registrado y analizado nuevas vulnerabilidades y el status de varias amenazas en los primeros seis meses de este año.
En este artículo resumimos la información que se puede ver más detallada en http://www.iss.net/documents/whitepapers/x-force_threat_exec_brief.pdf



El equipo de IBM X-Force para investigación y desarrollo de ISS ha detectado un incremento en el volumen y sofisticación de los códigos maliciosos, el aumento en el alquiler de "exploits" y una baja en el número de vulnerabilidades reportadas en comparación con la primera mitad de 2006.
X-Force destaca en el informe que la industria de la explotación como un servicio continúa prosperando en 2007. El reporte de 2006 de X-Force indicó que esos proveedores de administración de explotaciones habían comenzado a vender códigos de explotación desde el underground, encriptándolos de modo de que pudiesen piratearlos, vendiéndolos por importantes sumas de dinero a distribuidores de spam.



En 2007, esos proveedores de explotación han agregado la nueva práctica de "explotación por alquiler" a su repertorio. Alquilando una explotación, los atacantes pueden ahora testear técnicas con una pequeña inversión inicial, haciendo de este mercado subterráneo una muy atractiva opción para perpetradores maliciosos.

De acuerdo con el informe, los troyanos abarcan la más voluminosa categoría de malware en 2007, representando un 28 por ciento, en contraste con 2006, cuando la categoría más común era la de downloaders.

Troyano: archivos aparentemente legítimos conteniendo ocultos códigos maliciosos

Un **Downloader** es una pieza de bajo perfil de malware que es instalado por sí mismo pero que puede después bajar e instalar un agente malicioso más sofisticado.

El informe de estadísticas 2006 de X-Force predijo una continua alza en la sofisticación de objetivos, "de acuerdo a perfiles establecidos por los ciberatacantes", dijo Kris Lamb, director del team X-Force de IBM ISS. "Esto apunta directamente al alza en popularidad de troyanos que estamos verificando este año, cómo los troyanos son usados por los atacantes para lanzamiento sostenido de ataques dirigidos".
El uso de explotación por ofuscación continúa en alza en 2007, en una tentativa por dificultar la detección de intrusiones basadas en firma y productos de prevención para detectar ataques.
En 2006, X-Force reportó que aproximadamente el 50 por ciento del material de los hostings de sitios web estaba diseñado para infectar navegadores, los cuales eran ofuscados o "camuflaban" sus ataques. En la primera mitad de 2007, ese número ha alcanzado el 80 por ciento.

FOTO: http://www.sxc.hu/ - Jean Scheijen

Los ataques on line dirigidos continúan en ascenso

Considerando tendencias históricas, X-Force reporta un leve descenso en el número total de vulnerabilidades descubiertas en la primera mitad de 2007 versus la primera mitad de 2006. Un total de 3.273 vulnerabilidades fueron identificadas en la primera mitad de este año, marcando un descenso de 3,3 por ciento comparado con igual período de 2006.

Esta es la primera vez en la historia que el número de acceso a esas vulnerabilidades ha descendido en la primera mitad del año de acuerdo a los registros de X-Force, que fueron creados en 1997. Como siempre, el porcentaje de vulnerabilidades de alto impacto se ha elevado desde 2006 de un 16 a un 21 por ciento en la primera mitad de 2007.

X-Force apunta a una seria tendencia para explicar el descenso en acceso de vulnerabilidades en la primera mitad de 2007 versus el crecimiento exponencial de tendencias de vulnerabilidad observado en años anteriores. Primero, la monetización de vulnerabilidades y explotaciones ha ganado atención y madurez en el mercado underground; un gran porcentaje de vulnerabilidades son las que quedan sin revelar y están siendo usadas secretamente para pagar y obtener ganancias criminales.

Segundo, el incremento en el uso de "fuzzing" por investigadores de vulnerabilidades sobre los dos últimos años ha encubierto muchas de las más fáciles técnicas para encontrar vulnerabilidades.

"Como muchas tecnologías y software son expuestos al fuzzing, la industria comienza a alcanzar un punto de saturación en el descubrimiento de esas vulnerabilidades, contribuyendo al decrecimiento de todas las vulnerabilidades acceso", dijo Lamb.

Fuzzing es una técnica de investigación que randomiza datos; es provisto de un programa de software para generar fallos y por lo tanto detectar vulnerabilidades.

Finalmente, el número de errores de código común está bajando como resultado de la adopción de los proveedores de software y tecnologías más seguras, desarrollando ciclos de vida y prácticas más prudentes de código seguro.

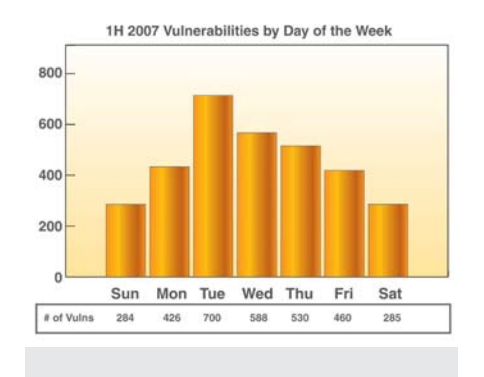
Una inesperada y similar tendencia en este reporte es que, por primera vez, el tamaño de los mensajes spam ha disminuido, en lugar de continuar en una estructura de crecimiento lineal. Esta baja corresponde con un descenso en el spam basado en imágenes.

Desde mediados de 2005, el spam basado en imágenes ha sido uno de los más grandes desafíos para las tecnologías anti spam, pero en la primera mitad de este año el porcentaje de spam basado en imágenes descendió del nivel de mediados de 2006 sobre un 30 por ciento. Hacia finales de 2006, el spam basado en imágenes ha representado más de un 40 por ciento de los mensajes spam.

"El descenso en el tamaño de los mensajes spam y el spam basado en imágenes es un resultado de medidas adoptadas por los spammers con nuevas técnicas, como las de spam basado en PDF y Excel, que cuentan con más éxito en la evasión y menos detección por parte de las tecnologías anti spam", dijo Lamb.

X-Force ha estado catalogando, analizando y desarrollando accesos de vulnerabilidades desde 1997. Con más de 33 mil vulnerabilidades catalogadas, es la más grande base de datos de vulnerabilidades en el mundo. Esto ayuda a los investigadores de X-Force a entender las dinámicas y elevar el descubrimiento de vulnerabilidades y accesos.

• El día en el que se revelaron mayor cantidad de vulnerabilidades fue el martes, con el 25 por ciento del total de vulnerabilidades dadas a conocer durante el primer semestre en 2007.

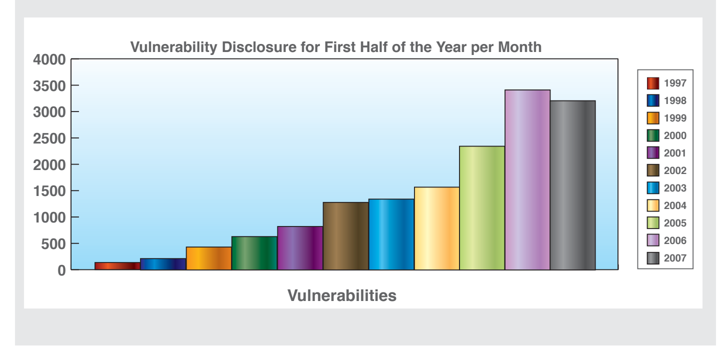


Vulnerabilidades

• Existen un total de 3.273 vulnerabilidades registradas en la primera mitad de 2007, registrándose una disminución de 3.3 por ciento respecto del mismo periodo en 2006. Esta es la primera vez en la historia de X-Force que estos números descendieron en el primer semestre.

• Enero fue el mes en el que más vulnerabilidades se registraron durante la primera mitad del año: un total de 600.

• En la tercera semana (enero 15-21) se registraron 149 vulnerabilidades siendo la semana más complicada del semestre.



• El Informe de Seguridad de IBM revela más de 210.000 nuevos códigos maliciosos.

• Los troyanos son el código malicioso de uso más popular, representando un 28%.

• El 80% del material de hostings de sitios web está diseñado para atacar navegadores.

• Leve descenso en el número total de vulnerabilidades descubiertas en la primera mitad de 2007 en relación con igual período de 2006. Sin embargo crece al 21% las vulnerabilidades de alto impacto.

Además de las vulnerabilidades catalogadas en la base de datos de X-Force, IBM ISS contiene servicios de filtrado, que son diseñados para entregar una visión que abarca todo el mundo del spam y ataques phishing. Con millones de direcciones de e-mail activas monitoreadas, ISS ha identificado numerosos avances en las tecnologías de spam y phishing usadas por los atacantes on line.

El reporte de X-Force también entrega las siguientes estadísticas claves de seguridad para la primera mitad de 2007, entre otras:

• Enero ha sido por lejos el más activo mes del año para vulnerabilidades, con 600 accesos.

• España ha tomado el lugar de Corea del Sur como el más grande generador de e-mails phishing, representando el 17,9 por ciento del volumen mundial.

• El porcentaje de vulnerabilidades que pueden ser explotadas remotamente ha crecido en la primera mitad de 2007 un 90 por ciento, versus el 88 por ciento de 2006.

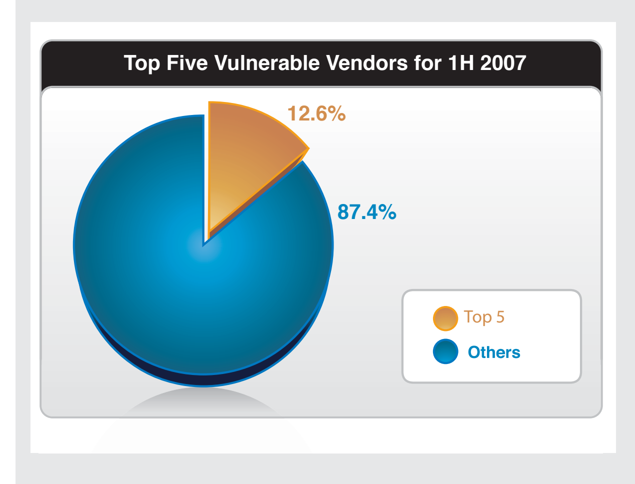
• El porcentaje de vulnerabilidades que permiten a un atacante ganar acceso al host des-

• La revelación de vulnerabilidades durante la primera mitad de 2007 se mantuvieron parejas con el mismo periodo del año anterior: 17.4 por ciento en 2007 comparado con 17.6 por ciento en 2006.

• El dos por ciento de las vulnerabilidades bajo el Common Vulnerability Scoring System (CVSS) fue evaluado como una vulnerabilidad crítica con un puntaje de 10.

• Los vendors más vulnerables durante el primer semestre de 2007 fueron Microsoft, Apple y Oracle.

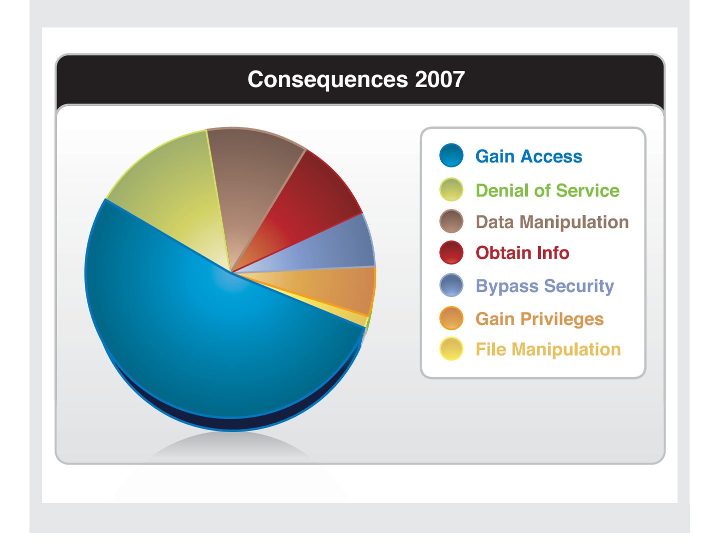
• Los cinco vendors más vulnerables registraron un total del 12.6 por ciento de todas las vulnerabilidades registradas.



• El 21 por ciento de las vulnerabilidades identificadas como productos de los principales vendors aún no tenían un parche para finales del primer semestre de 2007.

• El 90 por ciento de todas las vulnerabilidades descubiertas durante la primera mitad de 2007 pueden ser ejecutadas remotamente.

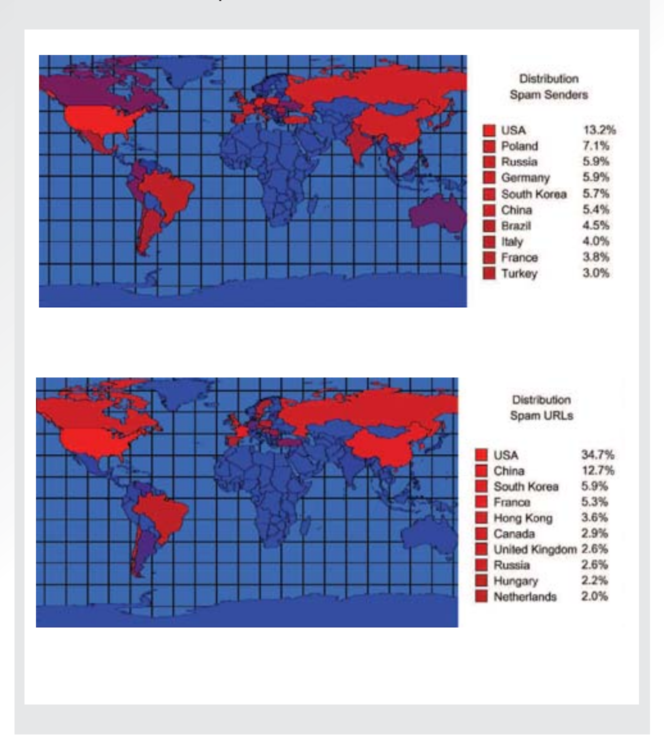
• Más de la mitad (51.6 por ciento) de las vulnerabilidades del primer semestre de 2007 permiten que el atacante tenga acceso al host luego de una explotación exitosa.



Spam y Phishing

• Estados Unidos, Polonia y Rusia es en donde se origina la mayor cantidad de spam del mundo.

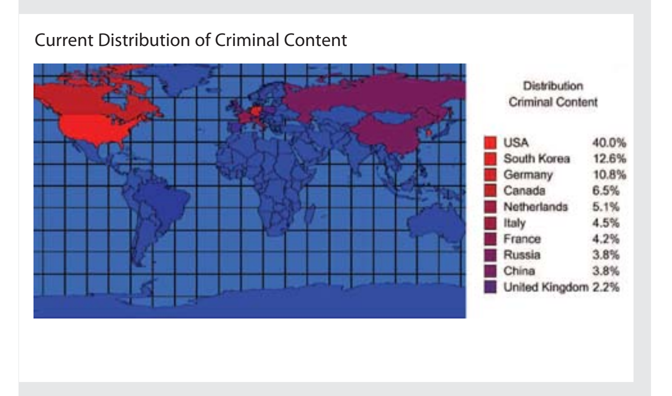
• Estados Unidos lidera el destino web final hacia donde redireccionan los productor promocionados a través de los mensajes de spam. Los Estados Unidos hostea más de un tercio de las Web relacionadas con el spam.



• Por primera vez, el tamaño de los mensajes de spam disminuyó en la primera mitad de 2007 en vez de continuar creciendo como lo venía haciendo. Este descenso se corresponde con la disminución del spam de imágenes.

• Casi la mitad de todos los sitios web fraudulentos están hosteados en Estados Unidos.

Current Distribution of Criminal Content

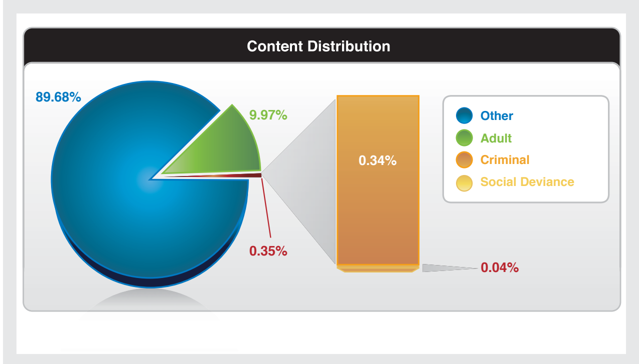


Contenido Web

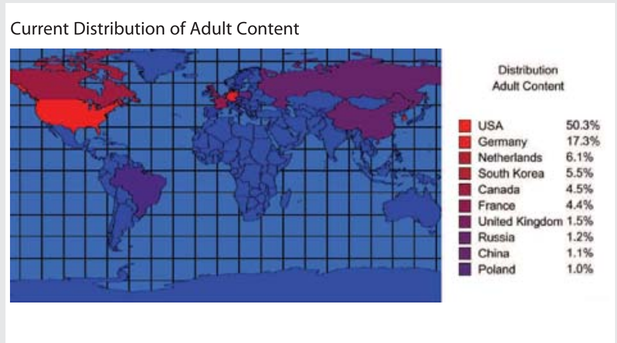
• El contenido "no deseado" disminuyó un 10 por ciento en el primer semestre de 2007, en comparación al 12.5 del mismo periodo de 2006.

• El 9.9 por ciento de los sitios web de Internet hostean contenido pornográfico o sexual.

• Estados Unidos continúa siendo el principal país en albergar contenido "no deseado" como violencia y crimen, pornografía y sexo, crimen tecnológico, y drogas ilegales.



Current Distribution of Adult Content



Conozca Internet Security Systems, una compañía IBM.

Internet Security Systems, Inc. (ISS), una compañía IBM, es el más confiado experto por empresas globales y gobiernos alrededor del mundo, que entrega productos y servicios que protegen contra toda amenaza de Internet. Indiscutible líder establecido desde 1994, ISS brinda prevenciones que reducen costos y riesgos empresariales. Los productos y servicios de ISS están basados en una inteligencia de seguridad proactiva conducida por el equipo de búsqueda y desarrollo X-Force la mayor autoridad mundial en cuanto a vulnerabilidad y búsqueda de amenazas. Con oficinas centrales en Atlanta, Internet Security Systems tiene operaciones con presencia local en Norte, Centro y Sudamérica, Asia, Australia, Europa y el Medio Este. Para más información visite www.iss.net

pués de ocurrida la explotación ha subido ligeramente también al 51,6 por ciento, desde el 50,6 por ciento en 2006.

• Actualmente, alrededor del 10 por ciento de Internet consiste en contenido no deseado como pornografía, crímenes, contenido para adultos o material desviado de la sociedad.

Para lo que queda de 2007 y 2008, x-Force espera observar una disminución del alza exponencial de divulgación de vulnerabilidades, la continua alza de objetivos y venta de malware como troyanos y una continua alza en las técnicas de ofuscación para amenazas basadas en Internet.

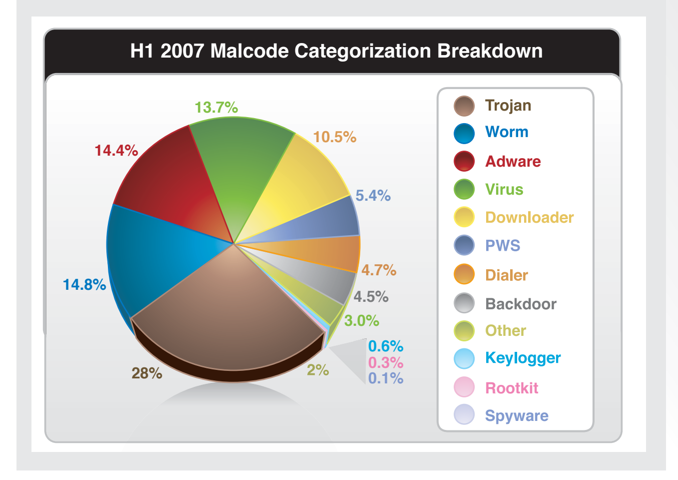
Para más tendencias en seguridad y predicciones de IBM acceda al documento completo "Ciber Ataques en alza: Reporte X-Force IBM de Mediados de Año" en: http://www.iss.net/x-force_report_images/2007. ●

Malcode

• La mayor amenaza del malware durante 2007 ha sido lejos el Troyano -61.161 variedades que representa el 28 por ciento de todo el malware.

• El malware más frecuente en Internet fue el Trojan.Win32.Agent - 26.573 variedades en la primera mitad de 2007 siendo el 43 por ciento de todos los Troyanos.

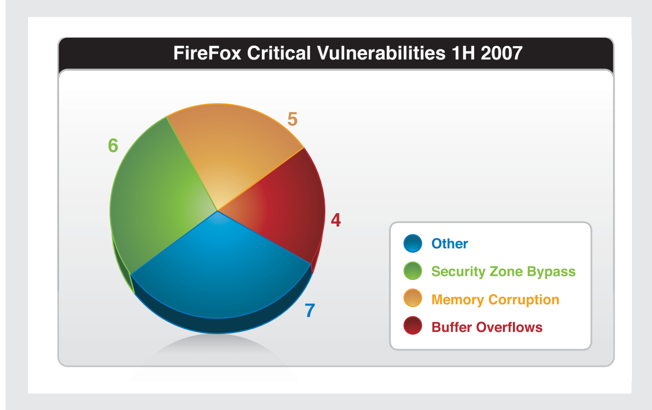
• El worm más común durante el primer semestre de 2007 fue Email-Worm.Win32.Mixor -12.120 variedades.

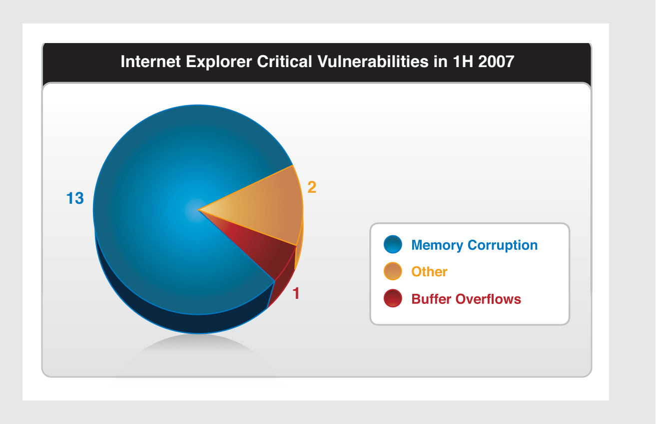


Web Browser Exploitation

• El exploit más popular usado en Internet para infectar los browsers con malware fue Visual Studio WMI Object Broker ActiveX.

• Aproximadamente el 80 por ciento de los exploits de Web son ofuscados de alguna forma, siendo JavaScript el vector ofuscador más común.





Fuente: Kaspersky

El spam en formato MP3

El correo basura continúa siendo un dolor de cabeza para varios. En la actualidad los elaboradores de correo spam, con el objeto de burlar la detección de los filtros antispam, recurrieron de manera activa a varios métodos innovadores para estos envíos: archivos en MP3.

Que las especies evolucionen naturalmente para sobrevivir no es algo que nos extrañe. Y tampoco ha de extrañarnos que lo mismo suceda en otros ámbitos. Salvando las diferencias, desde el momento en que se creó el término spam (devenido del "SPiced hAM") hasta el día de hoy, este malware ha mutado y se ha adaptado para poder seguir activo.

La novedad es la aparición del envío masivo de archivos de audio en formato MP3, conocido como "stock spam", el que viene diseñado para incrementar de manera artificial el precio de ciertas acciones bursátiles (stock, por su nombre en inglés) al publicitarlas.
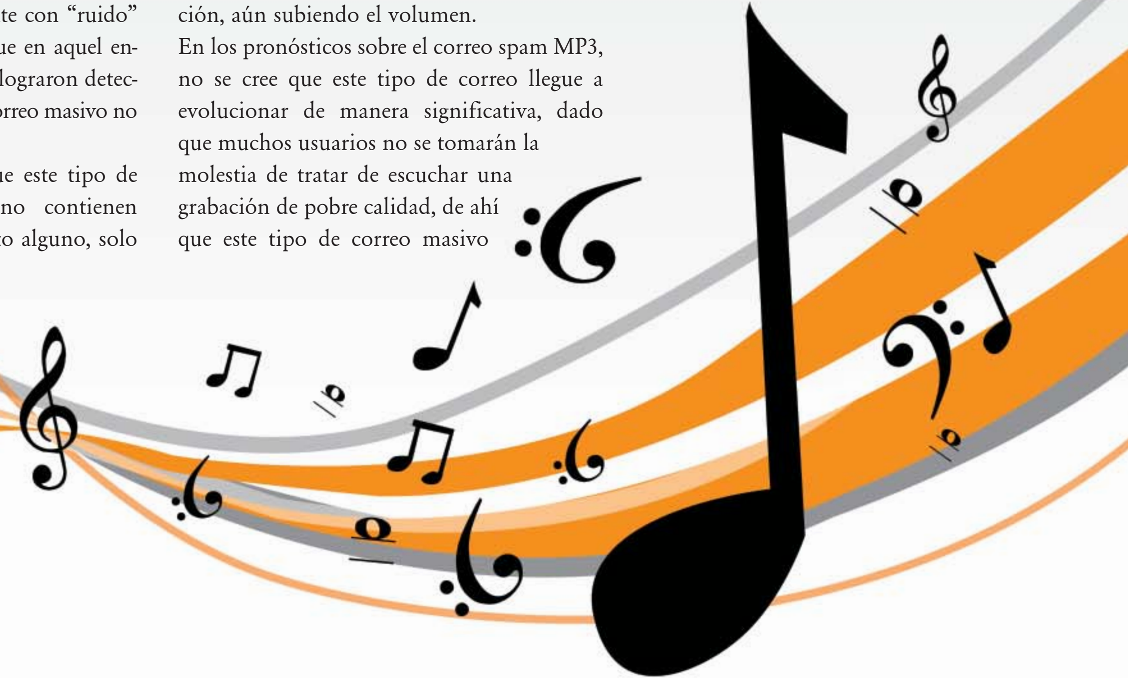
Este tipo de spam fue detectado por primera vez en agosto del año pasado usando archivos gráficos diseñados especialmente con "ruido" de fondo (en archivos .pdf), que en aquel entonces los filtros antispam no lograron detectar. Desde ese momento este correo masivo no ha parado de reproducirse.

La novedad es que este tipo de spam uno contienen texto alguno, solo una grabación adjunta que dura entre 25 y 33 segundos. Al abrir este archivo, el usuario oirá una voz femenina distorsionada publicitando acciones bursátiles de una compañía llamada Exit Only Inc. Éste es un intento de los elaboradores de correo spam para inflar los precios de las acciones y obtener ganancias por las ventas posteriores de acciones pertenecientes a la compañía publicitada.

Sin embargo, este envío masivo parece ser una prueba que ha fracasado debido a ciertas limitaciones técnicas. Para evadir los filtros antispam y lograr el menor tamaño posible de los mensajes, los elaboradores de spam han tenido que recurrir a grabaciones de muy baja calidad. Los usuarios que abren el archivo, tendrán dificultades para entender la grabación, aún subiendo el volumen.

En los pronósticos sobre el correo spam MP3, no se cree que este tipo de correo llegue a evolucionar de manera significativa, dado que muchos usuarios no se tomarán la molestia de tratar de escuchar una grabación de pobre calidad, de ahí que este tipo de correo masivo resulta muy poco eficaz.

"Los usuarios suelen enviarse archivos de sonido con contenidos divertidos; parecería que los elaboradores de spam están contando con que los usuarios crean que se trata de archivos que vale la pena escuchar. El usuario recibe un archivo MP3 y creyendo que se trata de algo divertido o interesante, lo abre. Pero los elaboradores de spam tienen limitaciones en el tamaño de la grabación que envían, razón por la cual la calidad de la misma es muy pobre. Es muy probable que veamos más envíos masivos de este tipo, pero no llegarán a tener un efecto real en nuestras estadísticas de correo spam", afirmó Andrey Nikishin, Director de Operaciones de Subcontratación de Seguridad Informática de Kaspersky Lab. ●



Leonel Iván Saafigueroa



CRYPTOME: "LA NSA ACCEDE A SISTEMAS MICROSOFT"

(http://cryptome.org/nsa-ip-update11.htm)

En el siguiente artículo (en inglés) podemos encontrar las distintas pruebas que confirman que la Agencia de Seguridad Nacional de USA puede llegar a tener acceso a cualquier sistema de Microsoft cuando lo desee. Cryptome, hace algún tiempo sigue la pista a las direcciones IP utilizadas por la NSA y afirman: "Los amplios rangos de IP publicados por Cryptome son utilizados por la NSA, por contratistas del sector privado que trabajan con la NSA y por agencias gubernamentales no estadounidenses amigas de la NSA para acceder tanto a sistemas independientes como a redes ejecutando productos de Microsoft".

UBUNTU 7.10 "MÁS BARATO Y MEJOR QUE WINDOWS VISTA"

Es de conocimiento público que el nuevo Windows Vista no está a la altura de las circunstancias, ni siquiera a la altura de su antecesor; es por ello que ahora es posible tener un sistema completamente libre, gratis, moderno y flexible para nuestras computadoras, si... "Gutsy Gibbon" el nuevo Ubuntu ya está disponible, y lo mejor de todo es que lo puedes descargar gratis desde su página de Internet o si tienes tiempo y puedes esperar un par de semanas es posible hacer el pedido por Internet y te lo envían gratis a tu casa. Lo has leído bien, como en sus versiones anteriores sin pagar un centavo podremos tener una copia original de esta maravilla de la programación. No es que quiera ser extremista pero puedo garantizarles que este sistema llegó a un nivel de desarrollo en donde podremos hacer todas las cosas que deseamos con una computadora. Como novedad trae integrado los nuevos efectos visuales de 3D de Compiz Fusion, además soporte para

DISPONIBLES LOS CLIENTES PARA LINUX Y MAC DE EVE ONLINE (http://www.eve-online.com/download/)

Los amantes de los juegos están de suerte, ya está disponible el cliente para Linux de EVE Online, un juego multijugador online masivo en el espacio. Este no es un cliente nativo para Linux, sino que hace uso de una versión especial de Cedega, el software de Transgaming, para hacer funcionar el juego. Hay que aclarar que no hay que pagar nada por esta versión de Cedega modificada para jugar a EVE Online, lo único que hay que pagar para jugar es la cuota mensual del servidor oficial. En la web oficial podéis encontrar las instrucciones de instalación paso a paso y la lista de requisitos hardware para jugar.

ENEMY TERRITORY: QUAKE WARS 1.2

(http://zerowing.idsoftware.com:6969/)

La nueva batalla entre stroggs y humanos se libra en Enemy Territory: Quake Wars, el juego desarrollado por Splash Damage sobre el universo Quake. Todos aquellos que tengan la versión Windows del juego podrán utilizarla también en su sistema Gnu-Linux favorito gracias al reciente cliente que ya alcanza la versión 1.2. El cliente completo o la actualización desde la versión previa los podéis descargar desde el tracker para bittorrent de Id Software.

Sobre el autor:

Leonel Iván Saafigueroas es analista de Sistemas, docente, radioaficionado (LU5ENP) y conductor del programa de radio libre hispano - Red-Handed Radio (www.red-handed-radio.com.ar).



los principales "winmodems", entre ellos los ADSL USB, X-Window "a prueba de fallos" por si hay un problema que impide que el sistema gráfico se inicie normalmente, un Kernel optimizado para ser ejecutado en entornos virtualizados, opciones para el ahorro de consumo de energía y reducción de la emisión de calor ideal para todos los dueños de notebooks. Otras novedades más estructurales incluyen: KDE 3.5.8, XFCE 4.4.1, GNOME 2.20, Pidgin 2.2.1 (para poder chatear en todas las redes de mensajería conocidas), Python 2.5.1, Kernel 2.6.22, OpenOffice.org 2.3.0 (la mejor suite de oficina libre hasta el momento).

DRIVERS 8.42.3 DE ATI (http://ati.amd.com/support/driver.html)
Poco a poco desde que AMD compro ATI, va trabajando en sus drivers para que sus tarjetas ATI funcionen mejor en sistema operativos Gnu-Linux, fruto de ello son los nuevos drivers 8.42.3 publicados recientemente. Ahora en esta nueva versión se incluye el soporte para AIGLX en toda la gama de tarjetas soportadas por el driver, además las tarjetas anteriores a la serie HD 2×00 se encuentran completamente soportadas. Se incluye soporte para X.org 7.3 y se ha mejorado el centro de control ATI Catalyst. AMD aún no recomienda estos drivers para ser incluidos en los paquetes para las distribuciones, pues pueden producir problemas de estabilidad. Los drivers recomendados para entornos estables siguen siendo los 8.40.4.Tanto la descarga como el anuncio oficial se pueden encontrar en la web de AMD, donde se pueden ver todos los detalles concretos que afectan al driver, tarjetas soportadas, etc.

SKYPE 2.0 BETA PARA LINUX CON SOPORTE DE VIDEO
(http://www.skype.com/download/skype/linux/beta/)
Una versión de este famoso cliente de telefonía esta disponible ahora para nuestro sistema Gnu-Linux favorito, entre las novedades que trae destaca la posibilidad de charlas con video. Un software muy famoso en su versión de Windows pero no tanto en el mundo Linux; de su versión anterior hubo pruebas suficiente de que accedía al archivo de usuarios de nuestro sistema, en fin... es el costo de hablar gratis por Internet con una aplicación propietaria, no digan que no les avise.

FEDORA 8 (http://fedoraproject.org/get-fedora)
Nueva versión de Fedora, esta la octava con nombre en código "Werewolf" fue anunciado con una inmensa lista de nuevas funcionalidades entre las que destacan características como Pulse Audio (para establecer el volumen de audio de cada aplicación por separado), para no ser menos que otras distribuciones incluye Compiz Fusion dando capacidad de un escritorio lo más avanzado posible. Otras novedades más estructurales incluyen: GNOME 2.20, KDE 3.5.8 y OpenOffice 2.3 que viene en el paquete de la distribución, por supuesto también está en el relativamente nuevo núcleo Linux 2.6.23. Pueden descargar los DVD de instalación desde la dirección de Internet de Fedora Project.

LIBERTAD-EN-PIXELES
(http://stage6.divx.com/Libertad-en-pixeles/videos/)

Todos aquellos interesados en descargar videos con temática de software libre, puede acceder a la siguiente dirección de stage6. En la misma encontrarán charlas de Richard Stallman, como también publicidades y datos curiosos sobre el fenómeno Linux y el Software Libre.

FOTO: http://www.sxc.hu/ - Pipp

BREVES



¿Qué pensás de la idea de formar parte de las mejores y más nuevas aplicaciones para Android? ¡Vos podés ser uno de ellos! Y para alentar tu esfuerzo, Google lanzó el Android Developer Challenge, el cual tiene 10 millones de dólares en premios para quien desarrolle la más novedosa aplicación móvil para la plataforma Android.

¿Cómo es?

El total del premio será distribuido equitativamente entre dos concursos:

- Android Developer Challenge I: Las presentaciones se aceptarán desde el 2 de enero hasta el 3 de marzo de 2008.
- Android Developer Challenge II: Esta parte será lanzada luego de que la primera plataforma esté disponible a mediados de 2008.

¡Creá la mejor aplicación!

Google acepta todo tipo de aplicaciones pero está en busca de las más novedosas y las que ayuden a los usuarios a utilizar mejor las capacidades de Android y de esta forma tener una mejor experiencia móvil. Estas son algunas de las sugerencias:

- Red social.
- Aplicaciones relacionadas con el entretenimiento.
- Productividad y colaboración como email, mensajes instantáneos, calendario, etc.
- Juegos.
- Noticias e información.
- Nuevas interfaces.
- Funcionalidades de mash-up.
- Servicios de localización de usuarios.
- Y todo lo que te emocione!

¿Cómo participar?

Primero hay que bajar el Android SDK, estar al tanto de los últimos desarrollos suscribiéndose al Android Developer Blog e ingresar a http://code.google.com/android/adc.html y seguir los pasos.

¿Qué es Android?

Android es un software abierto desarrollado por Google para dispositivos móviles que incluye un sistema operativo, middleware y aplicaciones key.

Lo que brinda Android es un conjunto de aplicaciones que incluyen un cliente de email, programa de SMS, calendario, mapa, browser, lista de contactos y más. Todas estas aplicaciones fueron escritas a través del lenguaje de programación Java.

Una de las ventajas es que los desarrolladores tienen completo acceso a algunas APIs usadas en las aplicaciones core. La arquitectura de las aplicaciones fue diseñada para simplificar el reuso de los componentes, cualquier aplicación puede publicar sus capacidades de forma tal que cualquier otra aplicación puede usar estas capacidades.

D-Link ahora soporta WPS

D-Link LatinAmérica anunció el nuevo soporte para la certificación WPS (Wi-Fi Protected Setup) vía actualizaciones en futuros lanzamientos de firmwares.

Esta Certificación está desarrollada a través de la Wi-Fi Alliance en aplicación con los dispositivos para el hogar y pequeñas empresas, lo que permite la comunicación entre los dispositivos que soporten 802.11a, 802.11b, 802.11g y 802.11n Draft 2.0. La certificación WPS aumenta la satisfacción de los usuarios proporcionando seguridad sobre sus dispositivos inalámbricos.

El soporte de D-Link para WPS ofrece una manera fácil y simple para configurar las redes con dispositivos inalámbricos que permitan WPS. Los productos que incorporan WPS de D-Link presentan dos opciones de autentificación y encriptación: PIN (Personal Identification Number) y PBC (Push Button Configuration).

Red Hat virtualizado

Red Hat Enterprise Linux 5.1 con virtualización integrada es el último lanzamiento del proveedor de soluciones de código abierto, el cual suma, además de funciones de virtualización, el ecosistema de implantación más amplio de la industria, abarcando sistemas autónomos, sistemas virtualizados, dispositivos y entornos informáticos de "nube" para Web Red Hat.

La virtualización de Red Hat Enterprise Linux 5.1 ofrece un soporte de servidores mucho más amplio que los productos de virtualización propietarios, y hasta el doble de rendimiento, el cual permite lograr una mayor consolidación de los servidores y elimina el principal obstáculo de una implementación más extensa de la virtualización.

La flexibilidad de implementación permite que los clientes pongan en uso una única plataforma, virtual o física, pequeña o grande, a lo largo de toda su empresa. Al ofrecer una plataforma que abarca la gama más amplia de servidores x86, x86-64, POWER, Itanium y mainframe, cantidad de núcleos o capacidad, los clientes logran una eficacia operativa y de costos. Red Hat Enterprise Linux 5.1 ofrece un mejor soporte para la virtualización de invitados de Microsoft Windows, logrando considerables mejoras en rendimiento en los guests de Windows XP, Windows Server 2000, 2003 y los invitados beta de Windows 2008.

Para mayor información acerca de Red Hat Enterprise Linux 5, visite www.redhat.com/rhel

Humor *por Severi*

